Gigamon®

GigaVUE Cloud Suite for Azure Secret and Top Secret Regions - Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.13

Document Version: 1.0

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc.

Trademark Attributions

Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners.

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054
408.831.4000

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
6.13	1.0	02/25/2026	The original release of this document with 6.13.00 GA.

Contents

GigaVUE Cloud Suite for Azure Secret and Top Secret Regions

The GigaVUE Cloud Suite for Azure Secret and Top Secret Regions option consists of the following components:

- **GigaVUE-FM fabric manager** - GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud.
- **GigaVUE V Series Proxy (Optional)** - GigaVUE® V Series Proxy manages multiple GigaVUE V Series Nodes and orchestrates the flow of traffic from GigaVUE V Series Nodes to the monitoring tools
- **GigaVUE V Series Nodes** - GigaVUE® V Series Node is a visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite Cloud using GRE or VXLAN tunnels, provided the cloud platform supports.

The images of all the fabric components are available in the Gigamon Customer Portal. For information about installing GigaVUE-FM in your enterprise data center, refer to the *GigaVUE-FM Installation, Migration, and Upgrade Guide*.

Prerequisites

This section lists the minimum requirements that are required for deploying the fabric components:

1. GigaVUE V Series Node requires a minimum of two network interfaces (NIC). Both can be on the same subnet or different subnets.
2. GigaVUE V Series Node requires a minimum of one Management interface (MGMT). Management interface is used for communicating between GigaVUE-FM and V Series Node.
3. GigaVUE V Series Node requires a minimum of one Data/Tunnel interface.
4. The minimum system requirements for V Series Proxy is 1CPU/1GB RAM.

Network Firewall Requirement

The following table lists the Network Firewall / Security Group requirements for GigaVUE Cloud Suite:

> **NOTE:** When using dual stack network, open the below mentioned ports for both IPv4 and IPv6.

GigaVUE FM

The following table specifies the inbound and outbound communication parameters—protocols, ports, and CIDRs—required for GigaVUE-FM to support secure access, registration, certificate exchange, and control-plane communication with associated components.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	443	Administrator Subnet	Allows GigaVUE-FM to accept Management connection using REST API. Allows users to access GigaVUE-FM UI securely through an HTTPS connection.
Inbound	TCP	22	Administrator Subnet	Allows CLI access to user-initiated management and diagnostics.

Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Node using REST API when GigaVUE V Series Proxy is not used.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Proxy using REST API.
Inbound	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive traffic health updates from GigaVUE V Series Nodes.
Inbound	TCP	9600	GigaVUE V Series Proxy	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Proxy.
Inbound	TCP	9600	GigaVUE V Series Node	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Node.
Inbound	UDP	2056	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive Application Intelligence and Application Visualization reports from GigaVUE V Series Node.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound (optional)	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Proxy.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Node.

Outbound	TCP	80	GigaVUE V Series Node	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Node.
Outbound	TCP	80	GigaVUE V Series Proxy	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Proxy.
Outbound	TCP	443	Any IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.

GigaVUE V Series Node

The following table outlines GigaVUE V Series Node’s network communication requirements, detailing protocols, ports, and CIDRs necessary for tunneling, management, diagnostics, and secure data transfer across connected components

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE-FM.
Inbound	TCP	8889	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	UDPGRE	4754	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from UDPGRE Tunnel.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Node to receive the ACME challenge requests from GigaVUE-FM.
Inbound	TCP	80	GigaVUE V Series Proxy IP	Allows UCT-V to receive the ACME challenge requests from the GigaVUE V Series Proxy.
Inbound (Optional - This port is used only for configuring AWS Gateway Load	UDP (GENEVE)	6081	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from AWS Gateway Load Balancer.

Balancer)				

Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM.
Outbound	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	UDP	2056	GigaVUE-FM IP	Allows GigaVUE V Series Node to send Application Intelligence and Application Visualization reports to GigaVUE-FM.
Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow Generation traffic to an external tool.
Outbound	UDP	8892	GigaVUE V Series Proxy	Allows GigaVUE V Series Node to send certificate request to GigaVUE V Series Proxy IP.
Outbound	TCP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	• echo request • echo reply	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V Series Proxy is not used.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	Tool IP	Allows to securely transfer the traffic to an external tool.

Giga VUE V Series Proxy (Optional)

The following table defines GigaVUE V Series Proxy’s network communication parameters, listing essential protocols, ports, and CIDRs for registration, certificate exchange, diagnostics, and control-plane traffic with GigaVUE-FM and V Series Nodes.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Proxy to receive the ACME challenge requests from the GigaVUE-FM.
Inbound	TCP	8300	GigaVUE V Series Node	Allows GigaVUE V Series Proxy to receive certificate requests from GigaVUE V Series Node for the configured params and provides the certificate using those parameters.
Inbound	TCP	8892	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate control and management plane traffic with GigaVUE V Series Node.

Ports for Backward Compatibility

Ensure to open these ports for backward compatibility when GigaVUE-FM is running version 6.10 or later, and the fabric components are on (n-1) or (n-2) versions.

GigaVUE V Series Node

The following table specifies the outbound communication requirement for GigaVUE V Series Node, detailing the protocol, port, and source CIDR used to send registration and heartbeat messages to the GigaVUE V Series Proxy during third-party orchestration.

Direction	Protocol	Port	Source CIDR	Purpose
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE V Series Proxy when GigaVUE V Series Proxy is used.

GigaVUE V Series Proxy(Optional)

The following table specifies the optional inbound communication parameter for GigaVUE V Series Proxy, detailing the protocol, port, and source CIDR required to receive security parameter requests from GigaVUE V Series Node during third-party orchestration.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive security parameter requests from GigaVUE V Series Node.

Inline V Series (Azure)

The Inline V Series solution provides an advanced, scalable, agentless traffic acquisition mechanism that integrates seamlessly into your network. By deploying V Series Nodes in inline mode, you can mirror and process traffic efficiently while ensuring the reinjection of production traffic without disruption.

In AWS and Azure environments, the Inline V Series solution leverages Gateway Load Balancers (GWLB) to enable efficient traffic handling and visibility. This feature ensures low-latency performance, making it ideal for continuous traffic inspection and monitoring. Designed for simplicity and operational efficiency, the Inline V Series allows you to gain deep insights into network activity while maintaining high performance in demanding network environments.

You can use this solution for forwarding inline traffic and traffic processing. When traffic reaches the Inline V Series Node, a copy of the packet is taken as out-of-band traffic. You can forward the copied traffic to a GigaVUE V Series Node for additional processing or directly to monitoring tools. During boot-up, the Inline V Series Node initializes with the default Inline application.

A Monitoring Session is required to:

- Tap the inline traffic
- Create a copy for out-of-band forwarding
- Send the traffic to the desired tools.

Inline V Series Deployment Types

Single Tier Deployment

You can use this deployment model when traffic has to be tapped, filtered, and directly sent to tools without any processing.

Multi-Tier Deployment

Use this model when you need to process traffic through GigaVUE V Series applications before forwarding it to the tools. The first tier taps the traffic, and the second tier processes it using the GigaVUE V Series applications and forwards it to the tools.

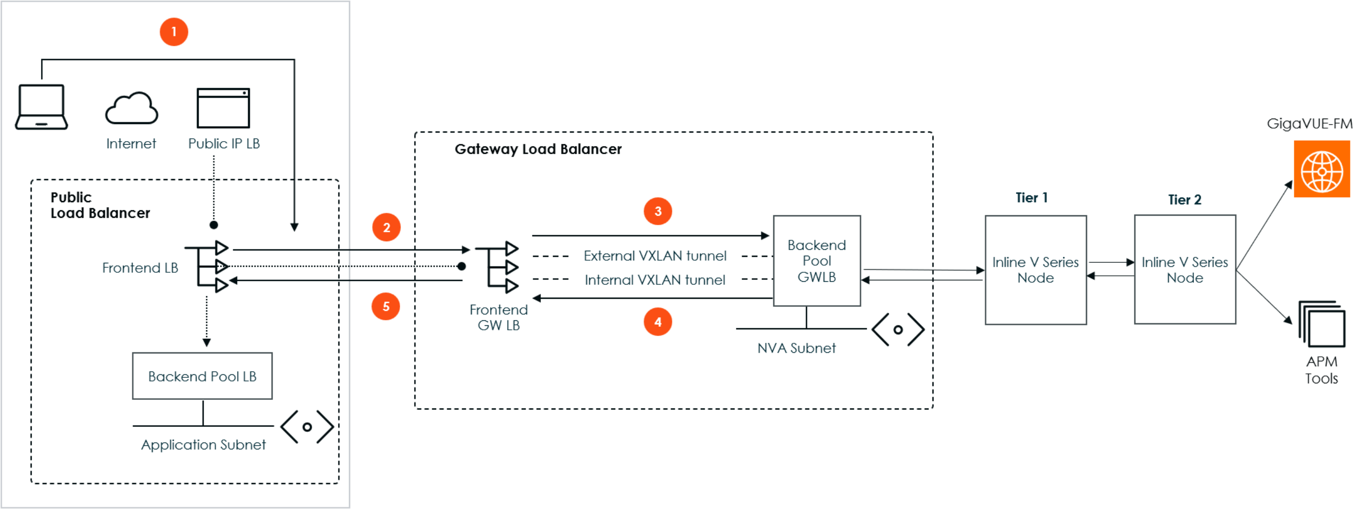
Architecture of Inline V Series Solution in Azure

Components required for configuring Inline V Series Solution in Azure:

- Application VNet
- Appliance VNet
- Public Load balancer
- Gateway Load balancer
- Inline V Series Node

Application VNet consists of multiple workload VMs, Public Load Balancer, Public IP Load Balancer, and Application Server in the Backend pool. The appliance VNet consists of Gateway Load Balancer, Inline V Series Node. Any traffic reaching the Gateway Load Balancer will be routed to the Inline V Series Node.

The below architecture diagram explains how the Inline V Series solution works:



Traffic from the internet to the application server:

1. The traffic from the internet is sent to the Public Load Balancer configured in Application VNet using an Public IP LB configuration.
2. This traffic is routed the Gateway Load balancer.
3. The Gateway Load Balancer in the Appliance VNet forwards the traffic to the Inline V Series Nodes. The following actions are performed in the Inline V Series Node:
   - Once the traffic reaches the Inline V Series Nodes, a copy of the packet is taken as out of band traffic.
   - The Out of Band traffic is forwarded to the GigaVUE V Series Node for further processing or it can be forwarded to the tools.
   - The Inline V Series swaps the IP address and the Mac of the packets, where the source and destination are interchanged. As a result the Inline V Series Node becomes the source and Gateway Load Balancer becomes the destination.

   NOTE: Packets sent from the Gateway Load Balancer will be VXLAN encapsulated and forwarded to the Inline V Series Nodes.

4. The inline traffic is sent back to the Gateway Load Balancer.
5. The Gateway Load Balancer forwards the inline traffic to the application servers in the Application VNet.

For a detailed workflow on acquiring traffic through the Inline V Series, refer to Deploy Inline V Series Solution in Azure.

Limitation

This solution can be implemented only to tap the North-South traffic.

Configure Custom Settings for Azure Secret and Top Secret Regions

This section explains how to configure GigaVUE Cloud Suite for Azure in Secret and Top Secret regions. These settings apply to users running Azure services in isolated environments where endpoints and regions are not publicly exposed.

GigaVUE-FM requires configuration options for service endpoint URLs, region settings, and CA certificates to connect to these isolated Azure environments.

> **NOTE:** This feature has been tested and validated only in IPv4-only environments.

Refer to the following sections for more details.

Configure Service Endpoints

This section provides steps to configure custom service endpoint URLs in GigaVUE-FM to enable connectivity with Azure Secret and Top Secret regions. These regions use isolated service endpoints that differ from those in Azure Commercial or Azure Government clouds.

To configure Service Endpoints:

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Custom Configuration**. The **Custom Configurations** page appears.
3. Select the **Custom Environment** tab and click **Create**.
4. On the **Configure Custom Environment** page, enter an **Environment Name** and the required service endpoint URLs:
   a. **resourceManagerEndpointUrl** - Base HTTPS endpoint that GigaVUE-FM can use to reach the Azure management/control plane APIs for your environment.
   b. **activeDirectoryEndpointUrl** - Base HTTPS endpoint for Azure Resource Manager (ARM) in your IL6 environment. All ARM API calls from GigaVUE-FM use this base URL.
   c. **managementEndpointUrl** - Base HTTPS endpoint for Azure Active Directory in your IL6 environment. GigaVUE-FM will use this to obtain access tokens.

> **Notes:**
>
> - GigaVUE-FM does not provide or auto-discover the required endpoint URLs. You must obtain the correct URLs from official Microsoft documentation or your Azure administrator.
> - Ensure that the URLs are valid HTTPS URLs.

5. Click **Save** to apply the custom environment configuration.

When creating or editing an Azure Credential in GigaVUE-FM, you can now select a custom environment that you have configured. Previously, only “**Azure**” and “**Azure US Government**” options were available. By choosing your custom environment, GigaVUE-FM will use the endpoints you specify, ensuring all connections align with your configuration. Refer to Create Azure Credentials for details.

Configure Custom Regions

This section explains how to define region entries that are not included in the SDK’s predefined list. Secret and Top Secret regions require manual addition so GigaVUE-FM can recognize and interact with them during Monitoring Domain setup.

To configure Custom Regions:

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Custom Configuration**. The **Custom Configurations** page appears.
3. Select the **Custom Region** tab and click **Create**.
4. On the **Configure Custom Region** page, enter the **Region Alias** and the exact **Region Name**. The Region Name can be user-defined (for example, East US or West US).
5. Click **Save**. The configured custom region will now be available for selection in the Monitoring Domain creation page. Refer to Create Monitoring Domain for details.

Import CA Certificate for Service Endpoints

Service endpoints in the secure regions may use TLS certificates signed by a Root CA that differs from the default trusted CAs in GigaVUE-FM. To establish secure HTTPS connections and validate server certificates, GigaVUE-FM must have the Root CA in its trust store. Importing the Root CA certificate ensures GigaVUE-FM can securely connect to the endpoints without certificate errors.

To Import Root CA into GigaVUE-FM Java Trust Store:

1. Obtain the required Root CA certificate file that signed the TLS certificate for your Azure Secret/Top Secret service endpoints.

2. Enter **"sudo keytool -keystore /usr/lib/jvm/java-17-openjdk-17.0.17.0.10-1.el8.x86_64/lib/security/cacerts -list"** in GigaVUE-FM. If prompted for a password, press Enter. The command lists the trusted Root CAs in the JDK trust store. Note the number of entries. The output includes a line such as: Your key store contains 146 entries. Here, the trust store contains 146 entries.
3. To import the Root CA into GigaVUE-FM, follow the steps listed below:
   a. Copy the Root CA into GigaVUE-FM, for example, to “/home/admin” or “/home/azureuser”.

```
[admin@GigaVUE-FM-6800 ~]$ ll
total 580
-rw------- 1 azureuser azureuser 4201 Nov 13 03:58 ca-chain.crt
```

   b. Import the certificate into JDK trust store:

      I. Run: "sudo keytool -import -alias <RootCAalias> -keystore /usr/lib/jvm/java-17-openjdk-17.0.16.0.8-2.el8.x86_64/lib/security/cacerts -file <RootCA.crt file>".

      II. When prompted for a password, enter the default trust store password: "**changeit**".

      III. The command displays certificate details (fingerprints, extensions) and prompts: Trust this certificate? [no]: Type **yes** and press Enter.

      IV. After successful import, it will display "Certificate was added to keystore".

      V. Repeat Step I to verify the Root CA is in the trust store. The entry count increases by one, and the Root CA appears in the list with the alias you specified, for example:

      .....

      Your keystore contains 147 entries

      .....

      userca, Nov 13, 2025, trustedCertEntry

      Certificate fingerprint (SHA-256): B0:0C:D7:F1:0B:A2:12:4D:BB:AB:70:90:61:4C:6C:5A:9A:69:D8:49:94:E2:2B:E5:CE:62:72:E1:8B:49:D1:62

      .....

4. Restart the CMS process to apply the certificate import:

```
sudo systemctl restart tomcat@cms.service
```

NOTE: You must repeat the import steps when upgrading GigaVUE-FM.

Deploy GigaVUE Cloud Suite for Azure Secret or Top Secret Regions

This chapter describes how to connect, launch, and deploy the fabric components of GigaVUE Cloud Suite for Azure Secret or Top Secret Regions.

Refer to the following topics for details:

- Create Azure Credentials
- Integrate Private CA
- Adding Certificate Authority
- Create Monitoring Domain
- Configure GigaVUE Fabric Components

Create Azure Credentials

You can monitor workloads across multiple Azure subscriptions within one monitoring domain. All the deployed GigaVUE fabric components are shared among many Azure subscriptions to reduce the cost. Earlier, each Azure subscription carried a set of GigaVUE fabric components.

- After launching GigaVUE-FM in Azure, the **Managed Identity** authentication credential is automatically added to the Azure Credential page as the default credential.
- You can only add the **Application ID with Client Secret** authentication credentials to the Azure Credential page.

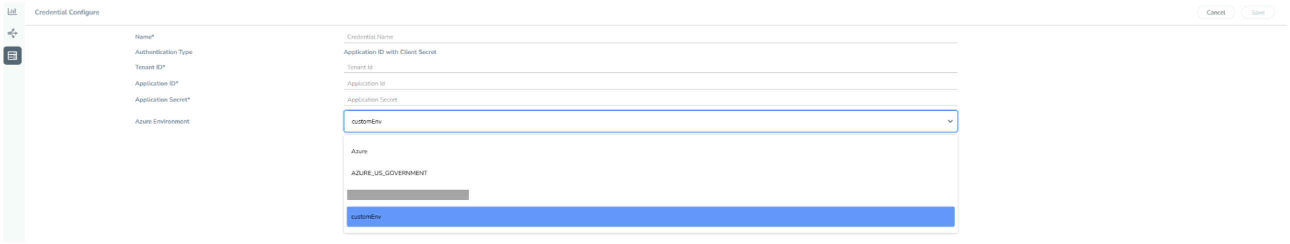
Prerequisite

You can configure a custom environment in Azure. For detailed instructions, refer to Configure Custom Settings for Azure Secret and Top Secret Regions.

To create Azure credentials,

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Credential**.
3. In the Azure Credential page, select **Add**.

   The **Configure Credential** wizard appears.



Name* Credential Name

Authentication Type Application ID with Client Secret

Tenant ID* Tenant Id

Application ID* Application Id

Application Secret* Application Secret

Azure Environment customEnv

[redacted]

4. Enter or select the appropriate information for the Azure credential:
   a. **Name:** An alias used to identify the Azure credential.
   b. **Authentication Type:**

      Application ID with Client Secret: Connection with Azure with a service principal. Enter the values for the following fields.

      - **Tenant ID**: A unique identifier of the Azure Active Directory instance.
      - **Application ID**: A unique identifier of an application in Azure platform.
      - **Application Secret**: a password or key to request tokens.

      For details on how to create service principal and assign custom roles, refer to Application ID with client secret.
   c. **Azure Environment:** Select an Azure environment where your workloads are located. For example, Azure_US_Government.
5. Select **Save**.

   You can view the list of available credentials in the Azure Credential page.

Integrate Private CA

You can integrate your own PKI infrastructure with GigaVUE-FM.
To integrate,

1. Generate a Certificate Signing Request (CSR).
2. Get a signature of the Certificate Authority (CA) on the CSR.
3. Upload it back to GigaVUE-FM.

Rules and Notes

- Always place the root CA in a separate file.
- When using multiple intermediate CAs, consider the following:
  - Include all intermediate CAs in a single file in the correct order.
  - Place the last intermediate CA in the chain at the top.
  - Place the preceding CAs in descending order.

Generate CSR

To create an intermediate CA certificate:

1. Go to ⚙ **> System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CSR**. The **Generate Intermediate CA Certificate** page appears.
3. Enter details in the following fields:
   - **Country:** Enter the name of your country.
   - **Organization**: Enter the name of your organization.
   - **Organization Unit:** Enter the name of the department or unit.
   - **Common Name**: Enter the common name associated with the certificate.
4. From the **Algorithm** drop-down list, select the desired encryption algorithm used to encrypt your private key.
5. Select **Generate CSR**.

The CSR is downloaded successfully.

Upload CA Certificate

Get the CSR signed from your Enterprise PKI or any public PKI and upload the signed intermediate CA certificate to GigaVUE-FM.

To upload the signed CA certificate to GigaVUE-FM:

1. Go to ⚙ **> System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CA**. The **CA Certificate** page appears.

3. From the **Actions** drop-down list, select **Upload CA**. The **Upload CA** pop-up appears.
4. Next to **Intermediate CA,** select **Choose File** to upload the signed intermediate CA certificate.
5. Next to **Root CA,** select **Choose File** to upload the corresponding root or intermediate CA.

The **CA Certificate** page displays the uploaded CA certificate.

Adding Certificate Authority

This section describes how to add CA Certificate chain Authority in GigaVUE-FM.

The CA Certificate chain List page allows you to add the root CA for the devices.

To upload the CA Certificate chain using GigaVUE-FM, follow these steps:

1. Go to **Inventory > Resources > Security > CA List**.
2. Select **Add**, to add a new Custom Authority.
   The **Add Certificate Authority** page appears.
3. In the **Alias** field, enter the alias name of the CA Certificate chain Authority
4. Use one of the following options to enter the CA Certificate chain Authority:
   - **Copy and Paste**: In the **Certificate** field, enter the certificate.
   - **Install from URL**: In the **Path** field, enter the URL in the format: <protocol>://<username>@<hostname/IP address>/<file path>/<file name>. In the **Password** field, enter the password.
   - **Install from Local Directory**: Select **Choose File** to browse and select a certificate from the local directory.
5. Select **Save**.

Create Monitoring Domain

A Monitoring Domain in GigaVUE-FM allows you to define and manage this connection. Once established, GigaVUE-FM can deploy and manage GigaVUE V Series Proxy, and GigaVUE V Series Nodes within your specified VNets and Resource Groups.

GigaVUE-FM connects to Azure using either an Application ID and Client Secret (Service Principal) or the Managed Service Identity (MSI) authentication method.

Prerequisite

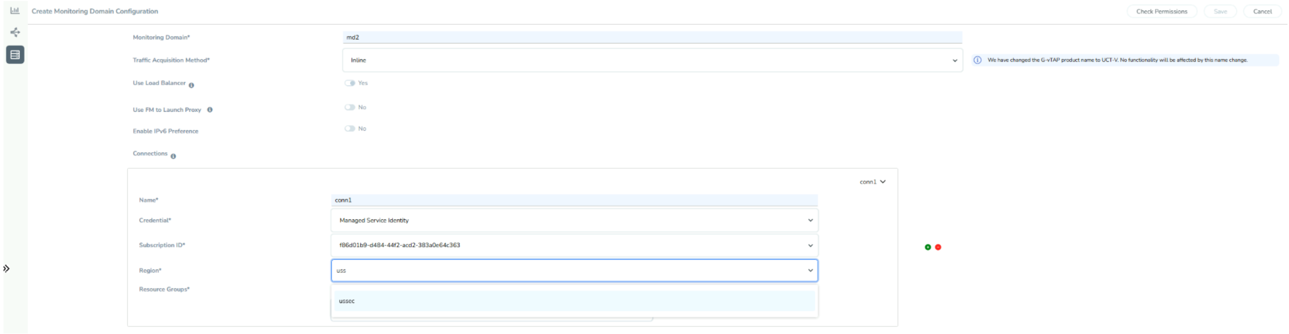
- Before configuring, you must establish a connection between GigaVUE-FM and your Azure environment.
- You configure a custom Region in Azure before creating a Monitoring Domain. For detailed instructions, refer to Configure Custom Settings for Azure Secret and Top Secret Regions.

To create an Azure monitoring domain in GigaVUE-FM,

1. Go to **Inventory > VIRTUAL > Azure**
2. Select **Monitoring Domain**.

   The **Monitoring Domain** page appears.
3. In the Monitoring Domain page, select **New**.

   The **Azure Monitoring Domain Configuration** wizard appears.



Monitoring Domain* md2

Traffic Acquisition Method* Inline

We have changed the G-vTAP product name to UCT-V. No functionality will be affected by this name change.

Use Load Balancer: Yes

Use FM to Launch Proxy: No

Enable IPv6 Preference: No

Connections

conn1

Name* conn1

Credential* Managed Service Identity

Subscription ID* f86d01b9-d484-44f2-acd2-383a0e64c363

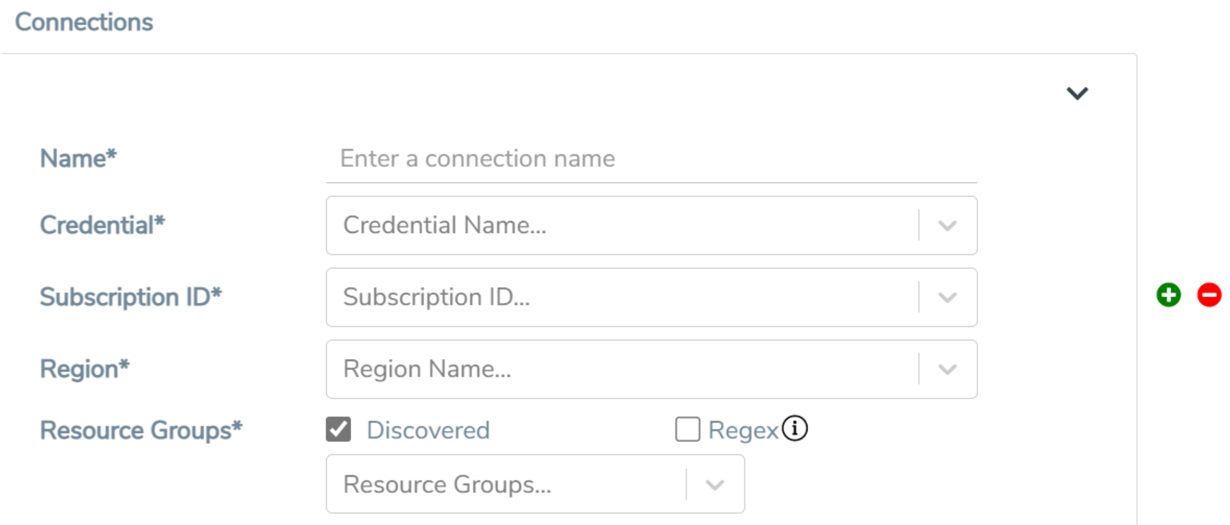
Region* uss

ussec

Resource Groups*

4. Enter or select the appropriate information for the Monitoring Domain:

   - **Monitoring Domain:** An alias used to identify the monitoring domain.
   - **Traffic Acquisition Method:** Select Inline as the Tapping method:
     - **Inline**: You can directly capture the inline traffic from the instances.
   - **Use FM to Launch Fabric:** Select **Yes** to Configure GigaVUE Fabric Components in GigaVUE-FM or select **No** to Configure GigaVUE Fabric Components .
   - **Connections:**



Connections

Name*	Enter a connection name	
Credential*	Credential Name...	
Subscription ID*	Subscription ID...	
Region*	Region Name...	
Resource Groups*	☑ Discovered	□ Regex ⓘ
	Resource Groups...	

     - A Monitoring Domain can have multiple connections, however only one connection can have **Managed Service Identity** as the **Credential**.
     - The connections in a monitoring domain can be a combination of multiple **Application ID with Client Secret** (Service Principal) accounts, or one **Managed Service Identity** and multiple **Application ID with Client Secret** (Service Principal) accounts.
     - Each connection can have only one **Subscription ID**.

   - **Name:** An alias used to identify the connection.
   - **Credential:** Select an Azure credential. For details, refer to Create Azure Credentials.
   - **Subscription ID:** A unique alphanumeric string that identifies your Azure subscription.
   - **Region:** Azure region for the monitoring domain. For example, West India.

- **Resource Groups:** Select the Resource Groups of the corresponding VMs to monitor.

  > **Notes:**
  >
  > - This field is not applicable if you select **Customer Orchestrated Source** as the **Traffic Acquisition Method**.
  > - When you remove and re-add a resource group in IAM, it won't appear in GigaVUE-FM automatically. To refresh the list and make the resource group selectable, reselect the Subscription ID from the drop down. This action triggers the UI to reload the resource groups associated with the selected subscription.

5. Select **Save**.

   The **Azure Fabric Launch Configuration** wizard appears.

> **Notes:**
>
> - Ensure that all V Series Nodes within a single Monitoring Domain are running the same version. Mixing different versions in the same Monitoring Domain may lead to inconsistencies when configuring Monitoring Session traffic elements.
> - Similarly, when upgrading a V Series Node, ensure that the GigaVUE-FM version is the same or higher than the V Series Node version.
> - You can only view and delete the existing configuration for GigaVUE V Series Node 1. You cannot perform any other actions on the existing configuration for GigaVUE V Series Node 1 as the features are deprecated from GigaVUE-FM.

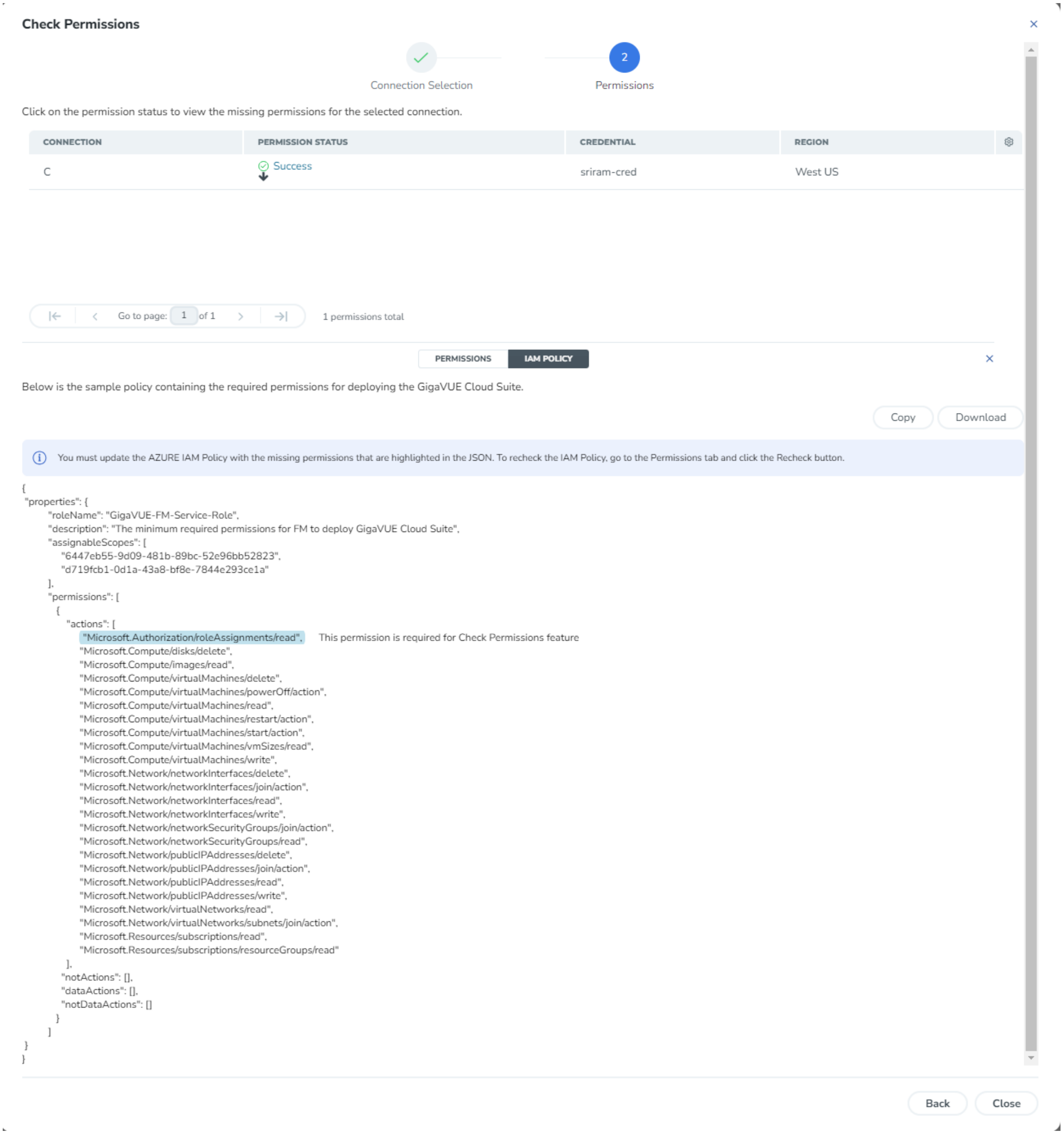
Check Permissions while Creating a Monitoring Domain

> **NOTE:** The Check Permissions feature is not available when the **Traffic Acquisition** Method is **vTAP**.

To check the permissions while creating a monitoring domain, follow these steps:

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Monitoring Domain**. The **Monitoring Domain** page appears.
3. Select **New**. The **Monitoring Domain Configuration** page appears.
4. Enter the details as mentioned in the Create Monitoring Domain section.
5. Select **Check Permission**. The **Check Permissions** widget opens.
6. Select the connection for which you wish to check the required permissions and then click **Next.**
7. Select the **Permission Status** tab to view the missing permissions. The **PERMISSIONS** tab lists the permissions required to run GigaVUE Cloud Suite for Azure.
8. Make sure to include all the permissions with Access Status as 'Denied' in the IAM policy.

The **IAM POLICY** tab lists the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite for Azure. You must update the Azure IAM policy with the missing permissions that are highlighted in the JSON. To recheck the IAM policy, go to the **PERMISSIONS** tab and selectthe **Recheck** button.



Click on the permission status to view the missing permissions for the selected connection.

CONNECTION	PERMISSION STATUS	CREDENTIAL	REGION
C	✓ Success	sriram-cred	West US

Below is the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite.

You must update the AZURE IAM Policy with the missing permissions that are highlighted in the JSON. To recheck the IAM Policy, go to the Permissions tab and click the Recheck button.

```
{
 "properties": {
        "roleName": "GigaVUE-FM-Service-Role",
        "description": "The minimum required permissions for FM to deploy GigaVUE Cloud Suite",
        "assignableScopes": [
           "6447eb55-9d09-481b-89bc-52e96bb52823",
           "d719fcb1-0d1a-43a8-bf8e-7844e293ce1a"
        ],
        "permissions": [
          {
            "actions": [
              "Microsoft.Authorization/roleAssignments/read",   This permission is required for Check Permissions feature
              "Microsoft.Compute/disks/delete",
              "Microsoft.Compute/images/read",
              "Microsoft.Compute/virtualMachines/delete",
              "Microsoft.Compute/virtualMachines/powerOff/action",
              "Microsoft.Compute/virtualMachines/read",
              "Microsoft.Compute/virtualMachines/restart/action",
              "Microsoft.Compute/virtualMachines/start/action",
              "Microsoft.Compute/virtualMachines/vmSizes/read",
              "Microsoft.Compute/virtualMachines/write",
              "Microsoft.Network/networkInterfaces/delete",
              "Microsoft.Network/networkInterfaces/join/action",
              "Microsoft.Network/networkInterfaces/read",
              "Microsoft.Network/networkInterfaces/write",
              "Microsoft.Network/networkSecurityGroups/join/action",
              "Microsoft.Network/networkSecurityGroups/read",
              "Microsoft.Network/publicIPAddresses/delete",
              "Microsoft.Network/publicIPAddresses/join/action",
              "Microsoft.Network/publicIPAddresses/read",
              "Microsoft.Network/publicIPAddresses/write",
              "Microsoft.Network/virtualNetworks/read",
              "Microsoft.Network/virtualNetworks/subnets/join/action",
              "Microsoft.Resources/subscriptions/read",
              "Microsoft.Resources/subscriptions/resourceGroups/read"
            ],
           "notActions": [],
           "dataActions": [],
           "notDataActions": []
          }
        ]
 }
}
```

You can use the **Copy** button to copy the permissions to the clipboard. Also, you can use the **Download** button to download the permission in JSON format.

NOTE: After updating the IAM Policy, it takes around 5 minutes for the changes to reflect on the Check Permissions screen.

Configure GigaVUE Fabric Components

You can use your own orchestration system to deploy the GigaVUE fabric components instead of using GigaVUE-FM to deploy the fabric components.

The GigaVUE fabric components register themselves with GigaVUE-FM using the information provided by you. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM. After launching the fabric component images in your orchestration system use the registration data provided in the sections below to deploy your fabric components to GigaVUE-FM. Health status of the registered nodes is determined by the heartbeat messages sent from the respective nodes.

This section provides step-by-step information on how to register GigaVUE fabric components using your own orchestration system or a configuration file.

Configure GigaVUE V Series Node and GigaVUE V Series Proxy

> **NOTE:** It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there are a large number of nodes connected to GigaVUE-FM or if you do not wish to reveal the IP addresses of the nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

To register GigaVUE V Series Proxy or node after launching the instance using a configuration file, follow the steps given below:

1. Log in to the GigaVUE V Series Proxy or Node.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following custom data.

```
Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <VPC ID>
        token: <Token>
        remoteIP: <IP address of the GigaVUE-FM> or
                  <IP address of the Proxy>
        remotePort: 443
```

> - You can register your GigaVUE V Series Node directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series node with GigaVUE-FM. If you wish to register GigaVUE V Series Node directly, enter the `remotePort` value as 443 and the `remoteIP` as *<IP address of the GigaVUE-FM>* or if you wish to deploy GigaVUE V Series node using GigaVUE V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as *<IP address of the Proxy>*.
> - Use only the default `user` and `password` details given in the custom data.

3. Restart the GigaVUE V Series proxy or node service.
   - GigaVUE V Series node:
     ```
     $ sudo service vseries-node restart
     ```
   - GigaVUE V Series proxy:
     ```
     $ sudo service vps restart
     ```

The deployed GigaVUE V Series proxy or node registers with the GigaVUE-FM.

After successful registration, the fabric components send heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the visibility node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the fabric components and if that fails GigaVUE-FM unregisters the fabric component and it will be removed from GigaVUE-FM.

Deploy Inline V Series Solution in Azure

NOTE: Click the following prompt to generate a quick deployment checklist for this topic.

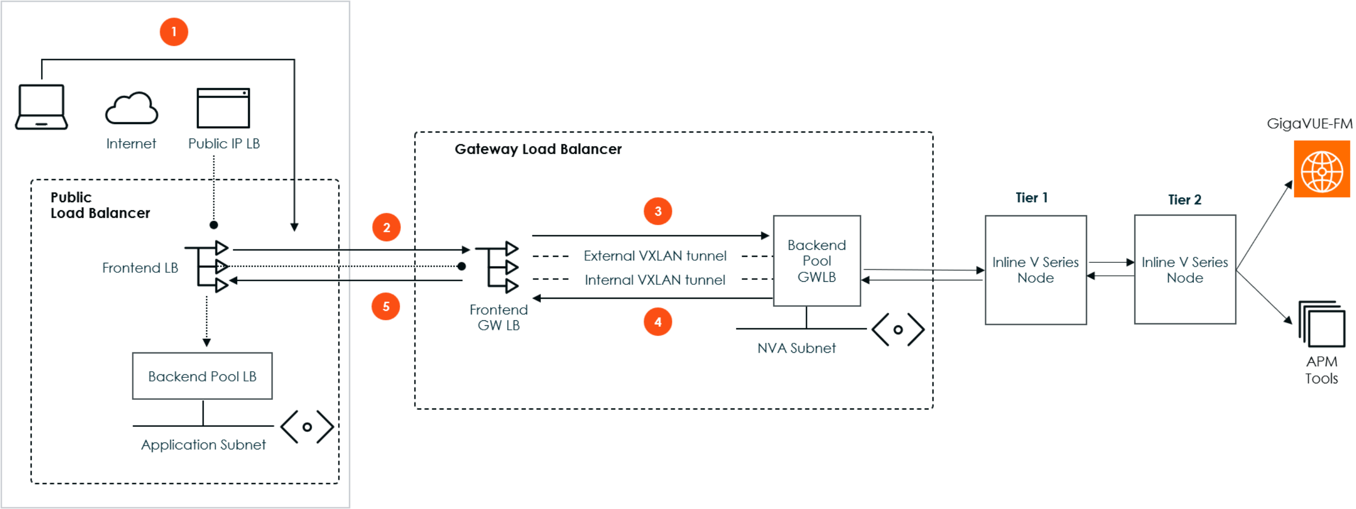
Create a comprehensive checklist based on the deployment steps outlined in the Deploy Inline V Series Solution in Azure topic.

This section outlines the work flow for acquiring traffic using Inline V Series Node and deploying GigaVUE Fabric Components using Third Party Orchestration. It provides instructions to configure traffic acquisition, processing, and forwarding to your desired destination.

Prerequisite

Ensure that you configure a custom environment and a custom region in Azure before creating a Monitoring Domain. For detailed instructions, refer to Configure Custom Settings for Azure Secret and Top Secret Regions.

Note: The work flow described in this section is based on the topology shown below. The approach for acquiring traffic depends on your specific requirements. Additionally, you can decide whether to route traffic through public load balancer based on your topology.



Refer to the following topics to deploy Inline V Series in Azure:

- Create a Resource Group
- Create Virtual Networks
- Create a Virtual Network Peering
- Create a Network Security Group
- Create a Load Balancer
- Install GigaVUE-FM on Azure
- Enable System Assigned Managed Identity
- Create Gigamon Custom Role
- Assign Role to Resource Group
- Assign Role to GigaVUE-FM Instance
- Create a GigaVUE-FM Token
- Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template
- Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node (Tier 1)
- Assign VMSS to GWLB Backend Pools
- Create Monitoring Domain
- Deploy GigaVUE V Series Nodes for Inline V Series Solution
- (Optional) Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node (Tier 2)
- Configure Monitoring session

Create a Resource Group

The resource group is a container that holds all the resources for a solution. Select an existing resource group or create a new resource group. For navigation steps and detailed instructions, refer to Create a resource group topic in the Azure Documentation.

> **NOTE:** We recommend creating a dedicated Resource Group for GigaVUE Visibility Fabric components such as GigaVUE-FM, V Series Nodes, Gateway Load Balancer, and others.

Create Virtual Networks

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. You can choose to:

- Select an existing VNet: When you choose an existing VNet, Azure automatically populates the Subnet and Public IP fields.
- Create a new VNet: To create a new VNet, follow the steps in the Create a virtual network topic in the Azure Documentation

> **NOTE:** We recommend setting up two separate virtual networks to support the GigaVUE Visibility Fabric. The first VNet (Viz_VNet) will host the GigaVUE visibility components such as GigaVUE-FM and V Series Nodes. The second VNet (App_VNet) will contain the virtual machines responsible for generating traffic.

Create a Virtual Network Peering

When workload virtual machines are distributed across multiple virtual networks, you must enable Virtual Network Peering between each workload VNet and the VNet hosting the GigaVUE V Series Node. This peering setup allows seamless communication between VNets within Azure.

To set up peering between the two VNets you created, refer to Manage a virtual network peering topic in Azure documentation.

Create a Network Security Group

Network Security Groups (NSGs) filter inbound and outbound traffic to subnets and network interfaces using security rules. You should configure the Network Security Group to allow GigaVUE-FM to communicate with the rest of the components. Select an existing network security group or create a new network security group. For navigation steps and detailed instructions, refer to Create a network security group topic in the Azure Documentation.

Create a Load Balancer

Gigamon deploys its solution as a Network Virtual Appliance positioned behind a Gateway Load Balancer. To ensure traffic flows through the V Series, it must be routed to the GWLB. You can achieve this routing either via a Standard Load Balancer or directly from a virtual machine's public interface. Microsoft recommends using a Standard Load Balancer for optimal integration.

Refer to the following sections for information on creating a Gateway Load Balancer and Standard Load Balancer:

Create a Gateway Load Balancer

Set up a Gateway Load Balancer (GWLB), which will later forward traffic to the Tier 1 V Series Node. Once deployed, the Tier 1 V Series Node will mirror packets from the workload virtual machines, enabling traffic visibility.

The following table lists the specific options you must select when creating a Gateway Load Balancer for an inline V Series deployment. For navigation steps and detailed instructions, refer to Create a Gateway Load Balancer topic in Azure documentation.

Parameters	Description	Mandatory field
Basics		
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group that you created	Yes
Name	Enter a valid name	Yes
Region	Select the region	Yes
SKU	Select **Gateway**	Yes
Type	Select **Internal**	Yes
Tier	Select **Regional** (default)	Yes
FrontEnd IP Configuration - Add a frontend IP configuration		
Name	Enter a valid name	Yes
IP Version	Select based on the requirement	Yes
Virtual Network	Select your virtual network	Yes
Subnet and IP Assignment	Select your subnet and choose **Dynamic** for assignment	Yes
Backend Pools - Add a backend pool		
Name	Enter a valid name	Yes
Virtual Network	Default	Yes

Parameters	Description	Mandatory field
Backend Pool Configuration	Select NIC	Yes
Gateway load balancer configuration		
Type	Choose **Internal and External**.	Yes
Internal and External Ports	Use default values **Note**: If you change the port values here, update the same ports in the **Custom data and cloud-init** field when creating the Virtual Machine Scale Set	Yes
NOTE: Add backend pool without IP Configuration (you will attach NICs later in this step Assign VMSS to GWLB Backend Pools).		
Inbound Rules - Add a load balancing rule		Yes
Name	Enter a valid name	Yes
IP Version	Select IPv4 or IPv6	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list	Yes
Backend Pool	Select an existing Backend pool from the drop-down list	Yes
Session Persistence	Select **None**	Yes
Health Probe	Select Create New and enter the following details: • Protocol - Select **HTTP** as the protocol • Port - Enter **8888** as the port • Path: /health • Interval - Enter 5 seconds as the approximate amount of time, in seconds	Yes
Idle timeout (minutes)	Leave default or adjust as required	Yes

(Optional) Create a Standard Load Balancer

NOTE: Routing traffic through a public load balancer is optional and applies only to the topology shown at the beginning of this document. Alternatively, you can route traffic to the Gateway Load Balancer from a VM that has an interface with a public IP.

The following table lists the specific options you must select when creating a Standard Load Balancer for an inline V Series deployment. For navigation steps and detailed instructions, refer to Create a Public Gateway Load Balancer topic in Azure documentation.

For details regarding traffic flow from Gateway Load Balancer to Standard Load Balancer, refer to Gateway Load Balancer topic in Azure documentation.

Parameters	Description	Mandatory field
Basics		
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group that you created	Yes
Name	Enter a valid name	Yes
Region	Select the region	Yes
SKU	Select **Standard**	Yes
Type	Select **Public** (validated type)	Yes
Tier	Select **Regional**	Yes
FrontEnd IP Configuration - Add a frontend IP configuration		
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
IP Type	Select **IP Address** as the IP type	Yes
Public IP address	Select the public IP address from the drop-down list. If required, you can create a new IP address	Yes
Gateway Load Balancer	Select the Gateway Load Balancer you created in the previous step to associate it with the frontend IP configuration	Yes
Backend Pools - Add a backend pool		
Name	Enter a valid name	Yes
Virtual Network	Select the same virtual network as the Standard Load Balancer —typically the App VNet—to ensure communication with the workloads.	Yes
Backend Pool Configuration	Select **IP Address**	Yes
IP Address	Specify the private IP address of the source/customer VM	
Inbound Rules - Add a load balancing rule		Yes
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list	Yes
Backend Pool	Select an existing Backend pool from the drop-down list	Yes
Protocol	Select **TCP** as the protocol	Yes
Port	Enter **80** as the port	Yes
Backend Port	You can configure the backend port to match the frontend port. Enter a value based on your traffic requirements	Yes
Health Probe	Select Create new and create a new Health Probe with TCP Protocol, Port 80, and 5-second attempt interval	Yes
Session Persistence	Select **None**	Yes

Parameters	Description	Mandatory field
Idle timeout (minutes)	Enter or select 4	Yes
Outbound Rules -		
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list.	Yes
Protocol	All	Yes
Idle timeout (minutes)	Enter or select 4	Yes
TCP Reset	Enabled	Yes
Backend Pool	Select an existing Backend pool from the drop-down list.	Yes
Port Allocation	Use the default number of outbound ports	Yes

Install GigaVUE-FM on Azure

To install GigaVUE-FM using the Azure Marketplace:

1. Go to Azure Marketplace and search for Gigamon. The latest version of Gigamon GigaVUE Cloud Suite for Azure appears. Click **Get it Now**.
2. In the pop-up window, select the **GigaVUE-FM (Fabric Manager) vX.XX - BYOL** option and click Continue.
3. Select the "**Want to deploy programmatically? Get started**" link.
4. Review the terms of service and the subscription name, and then select Enable. Click **Save**.
5. Verify the selected **Subscription** and **Plan**, then click **Create**.

6. Configure the GigaVUE-FM VM details. Most fields are pre-populated, but some require manual input. Enter the details as mentioned in Table 1: GigaVUE-FM Installation Steps. For detailed instructions, refer to Create a Linux virtual machine in the Azure in Azure Documentation.

Table 1: GigaVUE-FM Installation Steps

Field	Description
Basics	
Subscription	Select your subscription.
Resource Group	Select the Inline V Series Resource Group that you created.
System-assigned managed identity	Use a system-assigned managed identity when a resource needs to authenticate to other services, and you want the identity to be created and deleted with the resource. **Note**: If you update any role it would take more than an hour to reflect in GigaVUE-FM, however, if you use APP registration it would take between 5-10 minutes to update in GigaVUE-FM.
Virtual machine name	Enter a name for the VM.
Region	Select a region for Azure VM.
Availability Zone	Choose your availability zone
Security Type	To enable UEFI secure boot, select **Trusted launch virtual machines** from the drop-down list. Click **Configure security features** and ensure that the **Enable secure boot check box** is enabled.
Image	Select the latest GigaVUE-FM images. **NOTE:** You cannot select multiple images for a VM.
Size	Select the recommended instance type: GigaVUE-FM - **Standard_D4s_v3**
Authentication Type	We support only SSH public key authentication type • SSH public key o Enter the administrator username for the VM. o Enter the SSH public key pair name. • Password o Enter the administrator username for the VM. o Enter the administrator password. **NOTE:** The username "gigamon" is reserved for internal usage. Do not create a user with the name "gigamon"
Disks	

Field	Description
Disk Size	The required disk size for GigaVUE-FM is **2 x 40GB**.
Networking	
Virtual Network	Select the virtual network that you created.
Configure network security group	Select the network security group that you created.

> **NOTE:** Verify the summary before proceeding to create. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface.

After the deployment, navigate to the VM overview page, copy the **Public IP address**, and paste it in a new web browser tab.

If GigaVUE-FM is deployed in Azure, use **admin123A!!** as the password for the **admin** user to login to GigaVUE-FM. You must change the default password after logging in to GigaVUE-FM.

Enable System Assigned Managed Identity

Managed Identity (MSI) is a feature of Azure Active Directory. When you enable MSI on an Azure service, Azure automatically creates an identity for the service VM in the Azure AD tenant used by your Azure subscription.

To enable MSI on the VM running in GigaVUE-FM using the Azure portal, refer to Configure managed identities using the Azure portal in the Azure documentation.

Create Gigamon Custom Role

When you first connect GigaVUE-FM to Azure, you need the appropriate authentication for Azure to verify your identity and check if you have permission to access the resources that you are requesting. This is used for GigaVUE-FM to integrate with Azure APIs and to automate the fabric deployment and management.

> **IMPORTANT**: "Microsoft.Authorization/roleAssignments/read" permission is required for validating the required permissions. Ensure to include "Microsoft.Authorization/roleAssignments/read" permission in your IAM policy.

The ‘built-in’ roles provided by Microsoft are open to all resources. Refer to Create or update Azure custom roles topic in the Azure documentation to update the policy with the relevant IAM service.

After completing the configuration in the Basics, Permissions, and Assignable Scopes sections, copy the permissions listed below and paste them into the JSON code to create a custom role.

> **NOTE:** Ensure to assign the roles for the permissions listed below at the subscription level.

```
{
   "Name":"CustomRoleForInline",
   "description":"Minimum requirements for FM in inline tapping",
   "assignableScopes":[
      "/subscriptions/<Subscription ID>"
   ],
   "permissions":[
      {
         "actions":[
            "Microsoft.Resources/subscriptions/read",
            "Microsoft.Resources/subscriptions/resourceGroups/read",
            "Microsoft.Network/virtualNetworks/read",
            "Microsoft.Network/loadBalancers/read",
            "Microsoft.Network/loadBalancers/backendAddressPools/read",
            "Microsoft.Network/loadBalancers/backendAddressPools/backendPoolAddresses/read",
            "Microsoft.Compute/virtualMachineScaleSets/read",
            "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
            "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/read",
            "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ipConfigu
rations/read",
            "Microsoft.Compute/virtualMachines/read"
         ],
         "notActions":[],
         "dataActions":[],
         "notDataActions":[]
      }
   ]
}
```

> **NOTE:** Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly.

Assign Role to Resource Group

You can specify where the custom role is available for assignment such as a management group, subscription, or resource group and assign the created role to the resource group you created. In Azure, locate your newly created Role by navigating to “Management Groups” and selecting your subscription Id.

For further navigation and instructions to assign a role to your resource group, refer to the steps listed in **Update a custom role** and **Assignable scopes** sections of the Create or update Azure custom roles topic in the Azure documentation.

Assign Role to GigaVUE-FM Instance

You can assign the custom role you have created to GigaVUE-FM instance in Azure. For navigation path and detailed instructions, follow the steps listed in **Open the Add role assignment page**, **Select the appropriate role**, and **Select who needs access** sections of the Assign Azure roles using the Azure portal topic in the Azure documentation.

Create a GigaVUE-FM Token

GigaVUE-FM allows you to generate a token only if you are an authenticated user and based on your privileges in accessing the GigaVUE-FM. You can create multiple tokens if required.

To create a token in GigaVUE-FM, follow these steps:

1. Go to ⚙, select **Authentication** > **GigaVUE-FM User Management**. The **User Management** page appears.
2. In the **User Management** page, select **Tokens**.

   > **Note:** If you are a user with write access, then you can view a drop- down list under **Tokens**. Select **Current User Tokens** to create a token.

3. Select **New Token**.
4. Enter a name for the new token in the **Name** field.
5. Enter the days until the token is valid in the **Expiry** field.
6. Select the user group for which you are privileged to access GigaVUE-FM from the **User Group** drop-down list.
7. Select **OK** to generate a new token. The generated token appears on the **Tokens** page.
8. Select the token to copy and use it to authenticate the GigaVUE-FM REST APIs.
   a. Go to **Actions** > **Copy Token**.
   b. Paste the copied token in the required fields to complete authentication.

   > **Note:** You cannot view the generated token. You can only copy and paste the generated token.

Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template

The script given below will be essential for creating the VMSS, which uses this data to deploy the V Series node. This information is also required when configuring the Monitoring Domain in GigaVUE-FM.

Ensure you save these values in a secure location for reference in the upcoming steps. You can modify only the following parameters in the template:

- groupName
- subGroupName
- remoteIP
- Token

Custom Template:

> **NOTE:** Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly.

```
#cloud-config
write_files:
  - path: /etc/gigamon-cloud.conf
    owner: root:root
    permissions: '0644'
    content: |
      Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
        token: <token>

  - path: /etc/vseries-inline.conf
    owner: root:root
    permissions: '0644'
    content: ""
```

Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node (Tier 1)

V Series Nodes are created as part of a Virtual Machine Scale Set (VMSS) to allow scaling based on demand. This setup enables you to scale out or scale in the number of V Series Nodes as needed for each tier. Therefore, each tier will have a dedicated VMSS. The inline V

Series solution does not support standalone V Series Nodes that are not part of a scale set.

The following table lists the specific options you must select when creating a Virtual Machine Scale Set for an inline V Series deployment. For navigation steps and detailed instructions, refer to Create a Virtual Machine Scale Set topic in Azure documentation.

Parameters	Description	Mandatory field
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group	Yes
Virtual Machine Scale Set Name	Enter a valid name	
Region	Select a desired region	
Availability Zones	Choose if you want to use zones for high availability.	No
Orchestration		
Orchestration Mode	Select **Uniform** as the orchestration mode.	Yes
Security Type	Select **Standard** mode.	Yes
Scaling		
Scaling Mode	Choose **Autoscaling**.	Yes
Scaling Configuration	Click Configure to edit the scaling conditions.	Yes
Default Condition	Enter the Initial Instance Count as 0. **NOTE:** Once the Monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that you need to deploy in this Monitoring Domain.	Yes
Condition	Choose a metric-based scaling condition (For example, CPU usage, network traffic).	Yes
Metric Source	Select the metric (For example, Average CPU Percentage).	Yes
Scale out	Set conditions like greater than 70% for scaling up.	Yes
Scale in	Set conditions like less than 20%.	
Cooldown Period	Set a cooldown period to prevent rapid scaling.	Yes
Instance Details		
Instance Type	Choose **Standard_D4S_v4** as the VM size.	
Image	Select the GigaVUE V Series Node image.	
Authentication Type	Choose SSH public key.	
Username	Enter a user name. Do not use admin or gigamon.	
Networking		
Virtual Network	Select the required VNet.	Yes
Subnet Selection	Choose the appropriate subnet for Inline V Series Node.	Yes
NIC Configuration	GigaVUE V Series Node requires two NICs—one for management	Yes

Parameters	Description	Mandatory field
	and one for mirrored data traffic. To configure the Data NIC, add a second network interface, select the appropriate subnet and network security group (NSG), and enable Accelerated Networking.	
Management		

<table>
<tr><th>Parameters</th><th>Description</th><th>Mandatory field</th></tr>
<tr><td>Upgrade Mode</td><td>Choose <b>Automatic</b>.</td><td>Yes</td></tr>
<tr><td colspan="3"><b>Advanced</b></td></tr>
<tr><td>Custom data and cloud init</td><td>

Enter the Custom Template modified in step Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config files (**/etc/gigamon-cloud.conf** and **/etc/vseries-inline.conf**) and register with GigaVUE-FM using Third Party Orchestration.

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly.

```
#cloud-config
write_files:
  - path: /etc/gigamon-cloud.conf
    owner: root:root
    permissions: '0644'
    content: |
      Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
        token: <token>

  - path: /etc/vseries-inline.conf
    owner: root:root
    permissions: '0644'
    content: ""
```

Custom Data with Internal and External Ports

If you have modified the internal and external port values in the Gateway Load Balancer, use the following custom data:

```
#cloud-config
write_files:
  - path: /etc/gigamon-cloud.conf
    owner: root:root
    permissions: '0644'
    content: |
      Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        remoteIP: <IP address of the GigaVUE-FM>
```

</td><td>Yes</td></tr>
</table>

<table>
<tr><th>Parameters</th><th>Description</th><th>Mandatory field</th></tr>
<tr><td></td><td><pre><code>   remotePort: 443
      token: <token>

- path: /etc/vseries-inline.conf
  owner: root:root
  permissions: '0644'
  content: |
    tunnel: vxlan
    external_port : <Enter the port value>
    external_vni : <Enter the port value>
    internal_port : <Enter the port value>
    internal_vni : <Enter the port value&gt;</code></pre></td><td></td></tr>
</table>

Assign VMSS to GWLB Backend Pools

Identify the Gateway Load Balancer you created in Create a Load Balancer step. To attach the Data NIC of the VMSS to the Gateway Load Balancer:

1. In the Azure portal, navigate to the Gateway Load Balancer you created earlier.
2. From the main page, go to **Settings** and select **Backend Pool**.
3. Locate the Virtual Network (VNet) where your VMSS is deployed.
4. Click **+ Add** under **IP Configuration**.
5. In the pop-up window, search for the Data NIC associated with your VMSS.
6. Select the NIC and click **Add**.
7. Click Save to apply the changes.

Create Monitoring Domain

Azure Load Balancer launches and manages GigaVUE V Series Node that is registered with GigaVUE-FM.

To deploy GigaVUE V Series Node with Gateway Load Balancing in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > Azure** .
2. Select **Monitoring Domain**.
3. On the Monitoring Domain page, select **New**.
4. On the **Monitoring Domain Configuration** page, select **Inline** as the Traffic Acquisition method.

5. Enter the **Monitoring Domain** Name and the **Connection** Name as mentioned in the user data provided during the template launch in Azure. Refer to Advanced section in Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node (Tier 1).
6. (Optional) Turn on the **Use FM to launch Proxy** toggle to launch the GigaVUE V Series Proxy using GigaVUE-FM.

   > **NOTE:** You can use GigaVUE V Series proxy if GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network. GigaVUE V Series Proxy is a optional component.

   a. From the **Image** drop-down list, select the required image.
   b. From the **Size** drop-down list, select the instance size.
   c. For **Number of Instances**, specify the required number of instances.
   d. For **Management Subnet**:
      a. Select the **IP Address Type** as Private or Public.
      b. From the **Subnet** drop-down list, select the management subnet.
      c. Select **Add Subnet** under **Additional Subnets** to add additional subnets.
   e. Select **Add** under **Tags** to assign tags for resource identification.
7. Select **Save**.

Deploy GigaVUE V Series Nodes for Inline V Series Solution

When the Monitoring Domain is created successfully you will be navigated to the **Azure Fabric Launch Configuration** page in GigaVUE-FM automatically.

1. From the **Connections** drop-down list, select the required connection that you have configured.

   > **Note:**
   >
   > After configuring the Monitoring Domain and establishing the connection, update the **Default Condition** count in the following steps based on the number of GigaVUE V Series Nodes you want to deploy within the Monitoring Domain:
   >
   > - Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node (Tier 1)
   > - (Optional) Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node (Tier 2)
   >
   > Adjust the instance count in the scale set to match the required number of nodes for your deployment.

2. Select the required resource group from the **Resource Group** drop-down list.

3. From the **Gateway Load Balancer** drop-down list, select the Load Balancer configured in Azure.
4. Under **Node Groups**, you can configure multiple node groups based on the deployment use case.
   - **Inline Node Group:** This node group is used for the Inline V Series Node that is used for traffic acquisition.
     a. In the **Inline Node Group Name** field, enter a name for the node group.
     b. From the **Inline Auto Scaling Group** drop-down list, select the auto scaling group where you deploy the Inline V Series Node.
   - **(Optional) Node Group:** You can configure this section if you wish to process the traffic using GigaVUE V Series Node. You can add or delete node groups using the + and - buttons.
     a. In the **Node Group Name** field, enter a name for the node group.
     b. From the **Auto Scaling Group** drop-down list, select the VMSS created in Azure.
5. Select **Save**.

NOTE: You can configure a maximum of eight Node groups.

(Optional) Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node (Tier 2)

The Tier 2 V Series Node (Out-of-Band) processes mirrored traffic using GigaSMART operations to enrich and optimize data before forwarding it to the tool set. If only filtering is required, the Tier 1 V Series Node can handle it and send the traffic directly to the tool—eliminating the need for a Tier 2 node.

The following table lists the specific options you must select when creating a Virtual Machine Scale Set for Out-of-Band for an inline V Series deployment. For navigation steps and detailed instructions, refer to refer to Create a Virtual Machine Scale Set topic in Azure documentation.

Parameters	Description	Mandatory field
Availability Zones	Choose if you want to use zones for high availability.	No
Orchestration		
Orchestration Mode	Select **Uniform** as the orchestration mode.	Yes
Security Type	Select **Standard** mode.	Yes

Parameters	Description	Mandatory field
Scaling		
Scaling Mode	Choose **Autoscaling**.	Yes
Scaling Configuration	Click Configure to edit the scaling conditions.	Yes
Default Condition	Enter the Initial Instance Count as 0. **NOTE:** Once the Monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that you need to deploy in this Monitoring Domain.	Yes
Condition	Choose a metric-based scaling condition (For example, CPU usage, network traffic).	Yes
Metric Source	Select the metric (For example, Average CPU Percentage).	Yes
Scale out	Set conditions like greater than 70% for scaling up.	Yes
Scale in	Set conditions like less than 20%.	
Cooldown Period	Set a cooldown period to prevent rapid scaling.	Yes
Instance Details		
Instance Type	Choose **Standard_D4S_v4** as the VM size.	Yes
Image	Select the GigaVUE V Series Node image.	Yes
Authentication Type	Choose SSH public key.	Yes
Username	Enter a user name. Do not use admin or gigamon.	Yes
Networking		
Virtual Network	Select the required VNet.	Yes
Subnet Selection	Choose the appropriate subnet for V Series Node.	Yes
NIC Configuration	GigaVUE V Series Node requires two NICs—one for management and one for mirrored data traffic. To configure the Data NIC, add a second network interface, select the appropriate subnet and network security group (NSG), and enable Accelerated Networking.	Yes
Management		

Parameters	Description	Mandatory field
Upgrade Mode	Choose **Automatic**.	
Advanced		
Custom data and cloud init	Enter the Custom data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config files (**/etc/gigamon-cloud.conf** and register with GigaVUE-FM using Third Party Orchestration. **NOTE:** Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly.	Yes

```
#cloud-config
write_files:
  - path: /etc/gigamon-cloud.conf
    owner: root:root
    permissions: '0644'
    content: |
      Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        remoteIP: <IP address of the GigaVUE-FM>
        remotePort: 443
        token: <token>
```

Configure Monitoring session

When the **Traffic Acquisition Method** is **Inline**, the **UCT-I** application is available on the canvas by default. You can configure up to three tiers in a Monitoring Session and define multiple Sub Policies. Each Sub Policy can have its own ingress and egress tunnels and traffic processing applications.

Notes:

- You can configure a maximum of three tiers in a Monitoring Session.
- Tier 1 supports only Maps. Inline traffic is disabled and reserved for future use.
- You can configure a maximum of 8 Sub Policies in a Monitoring Session.
- Each Sub Policy can have its own Ingress Tunnels, Egress Tunnels, and Applications.
- Traffic from an out-of-band endpoint can either:
  - Pass through a Map and send to a tool using an Egress Tunnel.
  - (Optional) Send to the GigaVUE V Series Node of the next tier for further processing.

To configure the Monitoring Session for Inline V Series Solution:

Tier 1 Monitoring Session:

1. Perform one of the following options:
   - Create a new Monitoring Session. Refer to Create a Monitoring Session (Azure) for details.
   - On an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab.

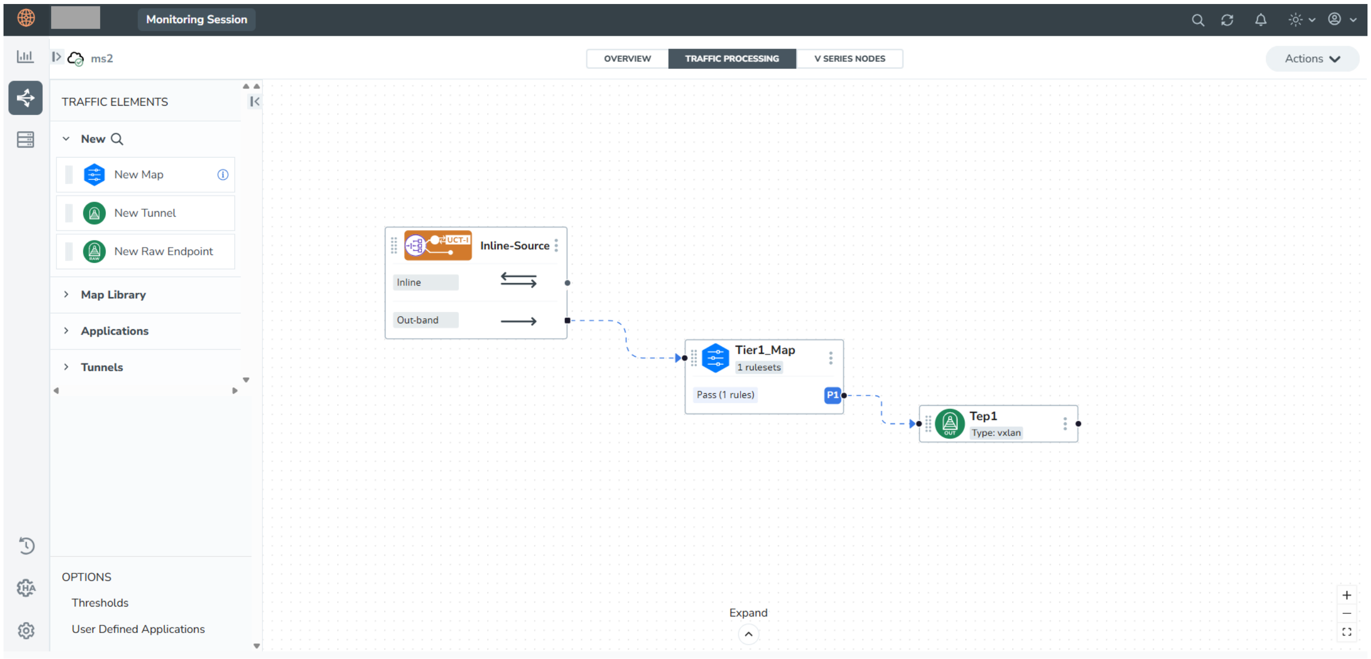
   The GigaVUE-FM Monitoring Session canvas page appears.

   When the **Traffic Acquisition Method** is **Inline**, the **UCT-I** application is available on the canvas by default.

2. Drag and drop the following items to the canvas as required for Tier 1 or Sub Policy 1:
   - Maps from the **new map** section. Refer to Create a New Map (Azure) for details.
   - Egress tunnels from the **new tunnel** section. When configuring Egress Tunnel, configure the **Remote Tunnel IP** if you intend to send the traffic directly from Tier 1 to the tool. Refer to Create Ingress and Egress Tunnels (Azure) for details.

     > **NOTE:** If sending traffic to Tier 2, Remote IP is optional. GigaVUE-FM will automatically add the remote IPs internally.

3. Now create a connection between the three tiles by dragging a line from the Inline-Source tile labeled “Out-Band” to the newly created Map and from Map to Egress tunnel.



Deploy Monitoring Session (Tier 1)

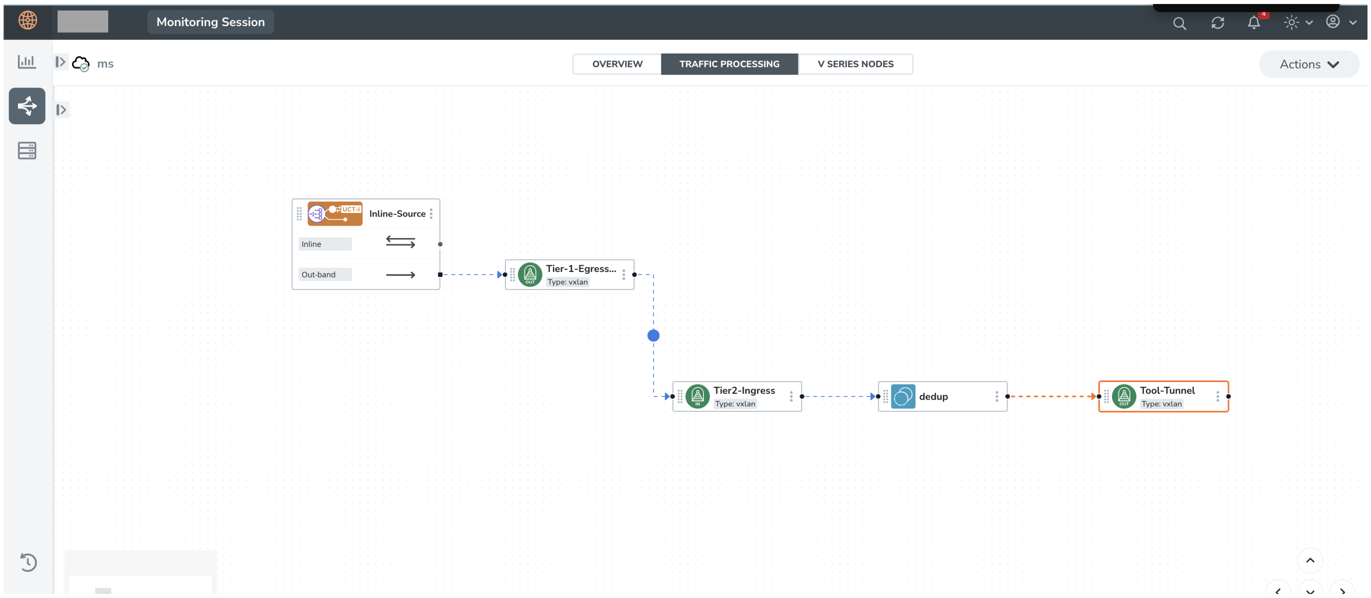
1. From the Actions drop-down list, select **Deploy**. The Deploy Monitoring Session pop-up appears.
2. Enter the following details:
   - In the **Policy Name** field, verify the auto-generated policy name or enter a custom name.
   - From the **Node Group** drop-down list, select the appropriate node group associated with this policy.
   - Under **Interface Mapping**, configure the interfaces:
     i. From the **Ingress - <Tunnel>** drop-down list, select the input interface.
     ii. From the **Egress - <Tunnel>** drop-down list, select the output interface.
3. Select **Deploy** the Monitoring Session.

To view the GigaVUE V Series Node associated with each Sub Policy, navigate to the **V SERIES NODES** tab and select a policy from the **Select a Sub policy** drop-down menu.

Tier 2 Monitoring Session (Optional):

You can send the filtered traffic to a Tier 2 V Series node, where GigaVUE-FM enriches and optimizes the data further.

1. In the same Monitoring Session canvas, drag and drop the following items to the canvas as required for Tier 2 or Sub Policy 2:
    - Ingress tunnel (as a source) from the **New** section. Refer to Create Ingress and Egress Tunnels (Azure) for details.
    - Maps from the **New Map** section. Refer to Create a New Map (Azure) for details.
    - GigaSMART apps from the Applications section. Refer to Add Applications to Monitoring Session (Azure).
    - Egress tunnels from the **new tunnel** section. Enter the **Remote Tunnel IP** address.
2. Create a link from the Ingress Tunnel to the Map or Application, and then connect it to the Egress Tunnel.
3. Create a direct link between the Egress Tunnel of Tier 1 and the Ingress Tunnel of Tier 2. The Blue Dot serves as an identifier to differentiate between tiers.
4. Repeat the above steps to configure a third tier, if required.



Deploy Monitoring Session Tier 1 to Tier 2

1. From the Actions drop-down list, select **Deploy**.

   The Deploy Monitoring Session pop-up appears.

2. For each Policy (Tier) configured in the Monitoring Session, enter the following details:

   - In the **Policy Name** field, verify the auto-generated policy name or enter a custom name.

   - From the **Node Group** drop-down list, select the appropriate node group associated with this policy.

   - Under **Interface Mapping**, configure the interfaces:

     i. From the **Ingress - <Tunnel>** drop-down list, select the input interface.

     ii. From the **Egress - <Tunnel>** drop-down list, select the output interface.

3. Select **Deploy** the Monitoring Session.

To view the GigaVUE V Series Node associated with each Sub Policy, navigate to the **V SERIES NODES** tab and select a policy from the **Select a Sub policy** drop-down menu.

What to do Next:

To view Monitoring Session Statistics and Dashboards for Inline V Series Solution, refer to:

- View Monitoring Session Statistics (Azure)
- Analytics for Inline V Series Solution (Azure)

Configure Monitoring Session

This chapter describes how to setup ingress and egress tunnels, maps, and applications in a Monitoring Session to receive and send traffic to the GigaVUE Cloud Suite V Series node. It also describes how to filter, manipulate, and send the traffic from the V Series node to monitoring tools.

Refer to the following sections for details:

- Create a Monitoring Session (Azure)
- Configure Monitoring Session for Inline V Series
- Create Ingress and Egress Tunnels (Azure)
- Create Raw Endpoint (Azure)
- Create a New Map (Azure)

- Add Applications to Monitoring Session (Azure)
- Interface Mapping (Azure)
- Deploy Monitoring Session (Azure)
- View Monitoring Session Statistics (Azure)
- Visualize the Network Topology (Azure)

Create a Monitoring Session (Azure)

You must create a Monitoring Domain before creating a Monitoring Session. Refer to Create Monitoring Domain.

GigaVUE-FM automatically collects inventory data on all target instances in your cloud environment. You can design your Monitoring Session to:

- Include or exclude the instances that you want to monitor.
- Monitor egress, ingress, or all traffic.

Target Instance

- When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds it to your Monitoring Session based on your selection criteria. Similarly, when an instance is removed, it updates the Monitoring Sessions.
- For the VPCs without UCT-Vs, targets are not automatically selected. In those cases, you can use Customer Orchestrated Source in the Monitoring Session to accept a tunnel from anywhere.

You can create multiple Monitoring Sessions within one Monitoring Domain.

To create a new Monitoring Session:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select **New Monitoring Session** to open the New Monitoring Session configuration page.

3. In the configuration page, perform the following:
   - In the **Alias** field, enter the name of the Monitoring Session.
   - From the **Monitoring Domain** drop-down list, select the desired Monitoring Domain or select **Create New** to create a Monitoring Domain.
     For details, refer to the Create a Monitoring Domain section in the respective cloud guides.
   - From the **Connections** drop-down list, select the required connections to include as part of the Monitoring Domain.
   - From the **VPC** drop-down list, select the required VPCs to include as part of the Monitoring Domain.
   - Enable the **Distribute Traffic** option to identify duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring.Distributed Deduplication is only supported on GigaVUE V Series Node version 6.5.00 and later.
4. Select **Save**.
   The Monitoring Session Overview page appears.

Monitoring Session Page (Azure)

The following table outlines the functional tabs available on the Azure Monitoring Session page, each designed to support specific aspects of network monitoring and session management:

Tab	Description
Overview	You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can also view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can filter the statistics based on the elements associated with the Monitoring Session. For more information, refer to View Monitoring Session Statistics (Azure).
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view and filter the connection details of the Monitoring Session. You can view the deployment status, number of targets, and targets source health. In the **Selection Status** section, you can view the VM status. The status indicates whether the VM is supported, not supported, selected, or not selected. When you hover over the status, a tooltip displays the reason for that status. **NOTE:** In the case of OVS Mirroring, the Sources tab also displays the Hypervisor details along with the Instances.
Traffic Acquisition	You can enable or disable Prefiltering, Precryption, and Secure Tunnel here. You can also create a Prefiltering and Precryption templates and apply them to the Monitoring Session. Refer to Configure Monitoring Session Options (Azure) . **Note**: Traffic Acquisition is only applicable for Monitoring Domain created with UCT-V as

Tab	Description
	Acquisition method.
Traffic Processing	You can view, add, and configure applications, tunnel endpoints, raw endpoints, and maps. You can view the statistical data for individual applications and also apply threshold templates, enable user defined applications, and enable or disable distributed De-duplication. Refer to Configure Monitoring Session Options (Azure).
V Series Nodes	You can view the V Series nodes associated with the Monitoring Session. In the split view, you can view details such as Node name, Health status (Configuration health + Traffic health), Host VPC, Management IP and Deployment Failure Message (if applicable). You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping (Azure).
Topology	Displays the fabric and monitored instances based on the connections configured in your network. You can select a specific connection to explore its associated subnets and instances in the topology view, offering a clear visualization of the monitored network elements. Refer to Visualize the Network Topology (Azure).

> **NOTE:** Ensure that the GigaVUE V Series Node and GigaVUE-FM are time synchronized or configure NTP time synchronization.

The Monitoring Session page **Actions** button has the following options. The Actions menu is placed common in all the tabs explained above.

Button	Description
Delete	Deletes the selected Monitoring Session.
Clone	Duplicates the selected Monitoring Session.
Deploy	Deploys the selected Monitoring Session.
Undeploy	Undeploys the selected Monitoring Session.

You can use the ▷ icon on the left side of the Monitoring Session page to view the Monitoring Sessions list. Click ≡ to filter the Monitoring Sessions list. In the side bar, you can:

- Create a new Monitoring Session
- Rename a Monitoring Session
- Hover over, click the check box of the required Monitoring Session(s) and perform bulk actions (Delete, Deploy, or Undeploy).

Configure Monitoring Session Options (Azure)

Configure Monitoring Session Options

In the Monitoring Session page, you can perform the following actions in the **TRAFFIC ACQUISITION** and **TRAFFIC PROCESSING** tabs:

- Enable Prefiltering
- Enable Precryption
- Apply Threshold Template
- Enable User-d efined applications
- Enable Distributed De-duplication

TRAFFIC ACQUISITION

To navigate to **TRAFFIC ACQUISITION** tab,

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select the required Monitoring Session from the list view on the left pane and select the **TRAFFIC ACQUISITION** tab.

You can perform the following actions in the **TRAFFIC ACQUISITION** page:

- Enable Prefiltering
- Enable Precryption

Enable Prefiltering

To enable Prefiltering:

1. In the **TRAFFIC ACQUISITION** page, go to **Mirroring > Edit Mirroring**.
2. Enable the **Mirroring** toggle button.
3. Enable **Secure Tunnel** option if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.
4. Select an existing Prefiltering template from the **Template** drop-down menu, or create a new template using **Add Rule** option and apply it. For details, refer to Create Prefiltering Policy Template.
5. Select the **Save as Template** to save the newly created template.
6. Select **Save** to apply the template to the Monitoring Session.

Enable Precryption

Consideration before you enable Precryption:

- To avoid packet fragmentation, change the option precryption-path-mtu in UCT-V configuration file (**/etc/uctv/uctv.conf**) within the range 1400-9000 based on the platform path MTU.
- Protocol version IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, ensure that the versions of GigaVUE-FM and the fabric components are 6.6.00 or above.

> **NOTE:** We recommend to enable the secure tunnel feature whenever the Precryption feature is enabled. Secure tunnel helps to securely transfer the cloud captured packets or Precryption data to a GigaVUE V Series Node. For more information, refer to *Secure Tunnels* in the respective GigaVUE Cloud Suite Deployment Guide.

To enable Precryption:

1. In the **TRAFFIC ACQUISITION** page, select **Precryption** tab and click **Edit Precryption**.
2. Enable the **Precryption** toggle button. Refer to Precryption™ topic in the respective cloud guides for details.

3. Apply Precryption to a few selective components based on the traffic:

   > **NOTE:** If you wish to use Selective Precryption, ensure that the versions of GigaVUE-FM and the fabric components are 6.8.00 or above.

   Applications:

   a. Select the **APPLICATIONS** tab.
      The **Pass All Applications** is enabled by default. If you wish to use selective Precryption, disable this option.
   b. Select any one of the following options from **Actions**:
      i. Include: Select to include the traffic from the selected applications for Precryption.
      ii. Exclude: Select to exclude the traffic from the selected applications for Precryption.
   c. Select **Add**. The **Add Application** widget opens.
   d. Select **csv** as the **Type**, if you wish to add the applications using a .csv file.
   e. Select **Choose File** and upload the file.
   f. Select **Manual** as the **Type**, if you wish to add the applications manually.
   g. Enter the **Application Name** and select + icon to add more applications.
   h. Select **Save**.

   L3-L4

   You can select an existing Precryption template from the **Template** drop-down list, or you can create a new template and apply it. For details, refer to Create Precryption Template for UCT-V.

4. Enable the **Secure Tunnel** option if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.

Validate Precryption connection

To validate the Precryption connection, follow the steps:

- To confirm it is active, navigate to the Monitoring Session **Overview** tab and check the Traffic Acquisition Options.
- Select **Precryption**, to view the rules configured.

Limitations

During Precryption, UCT-V generates a TCP message with the payload being captured in clear text. Capturing the L3/L4 details of this TCP packet by probing the SSL connect/accept APIs. The default gateway's MAC address is the destination MAC address for the TCP packet when SSL data is received on a specific interface. If the gateway is incorrectly configured, the destination MAC address is all Zeros.

TRAFFIC PROCESSING

To navigate to **TRAFFIC PROCESSING** tab:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select the required Monitoring Session from the list view on the left side of the screen and click **TRAFFIC PROCESSING** tab.

You can perform the following actions in the **TRAFFIC PROCESSING** page:

- Apply Threshold Template
- Enable User Defined Applications
- Enable Distributed De-duplication
- Tool Exclusion

Apply Threshold Template

To apply threshold:

1. In the **TRAFFIC PROCESSING** page, select **Thresholds** under **Options** menu.
2. You can select an existing threshold template from the **Select Template** drop-down list, or you can create a new template using **New Threshold Template** option and apply it.
   For more details on Threshold Template, refer to the Traffic Health Monitoring section.
3. Select **Save** to save the newly created template.
4. Select **Apply** to apply the template to the Monitoring Session.

> **NOTE:** You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

You can also view the related details of the applied thresholds, such as Traffic Element, Metric, Type, Trigger Values, and Time Interval in the **Threshold** window. Select **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User Defined Applications

To enable user defined application:

1. In the **TRAFFIC PROCESSING** page, click **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button.
3. Add from the existing applications or create new User-Defined Application from the **Actions** drop-down. Refer to User Defined Application.

Enable Distributed De-duplication

In the TRAFFIC PROCESSING page, click **Distributed De-duplication** under **Options** menu. Enabling the Distributed De-duplication option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. Refer to Distributed De-duplication.

> **Notes:**
>
> - Distributed De-duplication is only supported on V Series version 6.5.00 and later.
> - From version 6.9.00, Traffic Distribution option is renamed to Distributed De-duplication.

Tool Exclusion

Tool Exclusion helps prevent traffic loops by ensuring monitoring tools are not mistakenly selected as traffic targets during Automatic Target Selection (ATS). This feature is available only when the traffic acquisition method is VPC Traffic Mirroring.

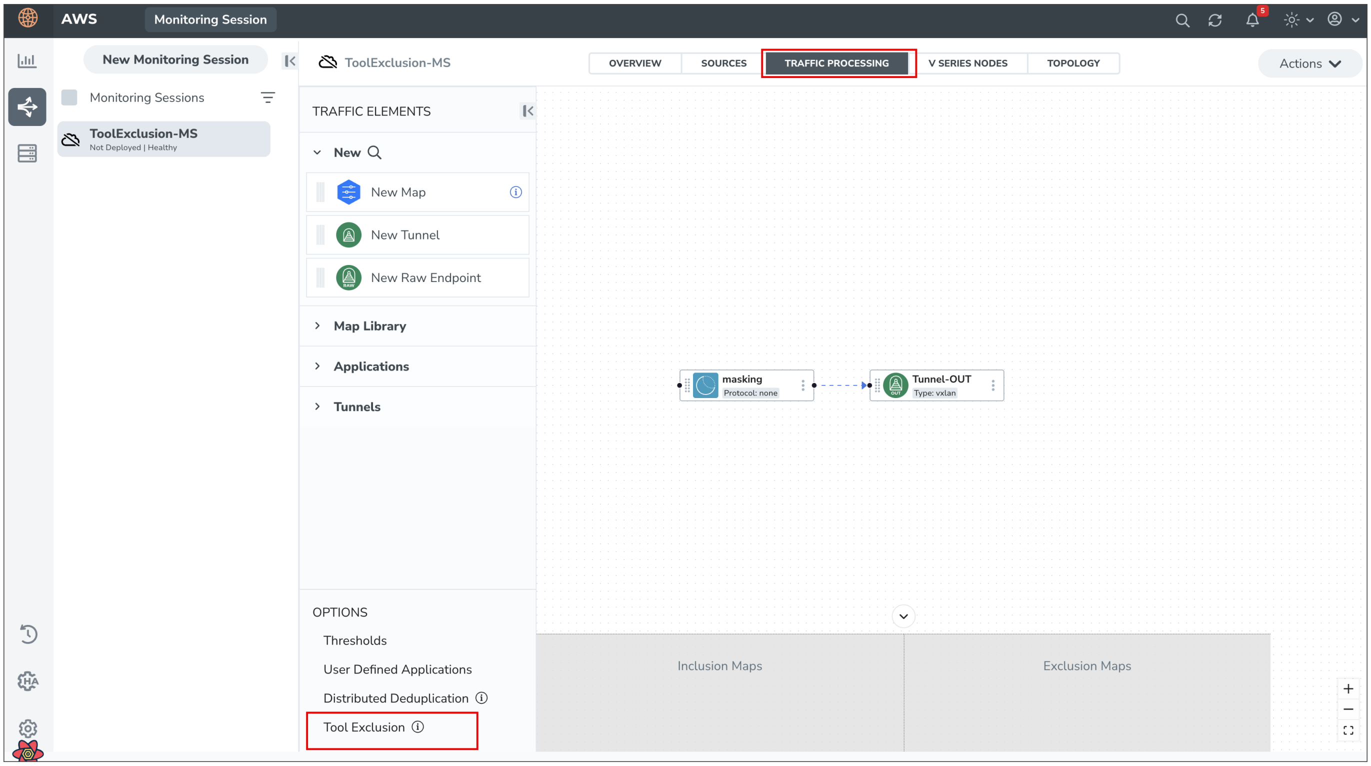
You can exclude tool instances using either of the following methods:

1. **Using AWS Tag Key**

   During deployment, apply the AWS tag key **GigamonExclude:Value** (Any Value) to any instance that acts as a monitoring tool. This tag ensures the system automatically excludes these instances from ATS.

2. **Using the Tool Exclusion Feature in UI**

   During deployment, if the same instance IP is configured as both source (ingress) and tool (egress),the system prompts you to manually identify and exclude tools. Also, you can use the **Tool Exclusion** option to include or exclude tools and targets manually.



Create Ingress and Egress Tunnels (Azure)

Traffic from the GigaVUE V Series Node is distributed to tunnel endpoints in a Monitoring Session. A tunnel endpoint can be created using a standard L2GRE, VXLAN, UDPGRE, UDP, or ERSPAN tunnel.

Notes:

- GigaVUE-FM lets you configure ingress tunnels in a Monitoring Session when you use the Traffic Acquisition Method UCT-V.
- The maximum number of links that can egress from any endpoint in V Series is four.

Create a new tunnel endpoint

To create,

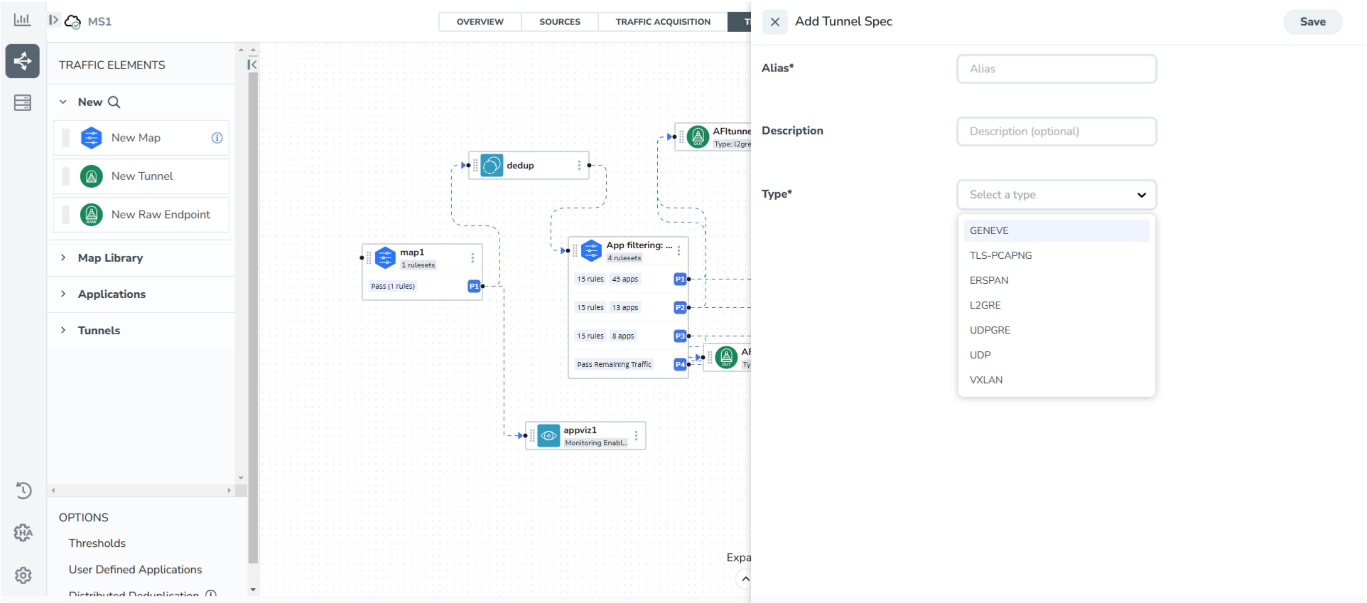
1. Perform one of the following and navigate to the **TRAFFIC PROCESSING** tab:
   - Create a new monitoring session
   - Select **Actions > Edit** on an existing monitoring session.

   The GigaVUE-FM Monitoring Session canvas page appears.

2. On the left pane of the canvas, select the icon to view the traffic processing elements.
3. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace.

   The **Add Tunnel Spec** quick view appears.
4. Enter the **Alias**, **Description**, and **Type** details.

   For details, refer to Details - Add Tunnel Specifications table.
5. Select **Save**.



To delete a tunnel, select the menu button of the required tunnel and select **Delete**.

Apply a threshold template to Tunnel End Points

1. Select the menu button of the required tunnel endpoint on the canvas and click **Details**.
2. In the quick view, go to the **Threshold** tab.

   For details on creating or applying a threshold template, refer to the Monitor Cloud Health topic in the respective Cloud guides.

You can use the configured Tunnel End Points to send or receive traffic from GigaVUE HC Series and GigaVUE TA Series. Provide the IP address of the GigaVUE HC Series and GigaVUE TA Series as the Source or the Destination IP address as required when configuring Tunnel End Points.

After configuring the tunnels and deploying the Monitoring Session, you can view the number of ingress and egress tunnels configured for a Monitoring Session. Select the numbers of tunnels displayed in the **OVERVIEW** tab to view the tunnel names and their respective **ADMIN STATUS** and **HEALTH STATUS**.

Table 1: Details - Add Tunnel Specifications

Field	Description	
Alias	The name of the tunnel endpoint.	
Description	The description of the tunnel endpoint.	
Admin State **Note**: This option appears only after the Monitoring session deployment.	Use this option to send or stop the traffic from GigaVUE-FM to the egress tunnel endpoint. Admin State is enabled by default. You can use this option to stop sending traffic to unreachable or down tools. Each egress tunnel configured on the GigaVUE V SeriesNode has an administrative state that enables GigaVUE-FM to halt the tunnel's traffic flow. GigaVUE-FM only disable the tunnels when it receives a notification via REST API indicating that a tool or group of tools is down. **Note**: This option is not supported for TLS-PCAPNG tunnels.	
Type	The type of the tunnel. Select from the options below to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.	
VXLAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **Note**: In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to configure secure tunnels on your physical device conveniently. For details, refer to Secure Tunnels.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	VXLAN Network Identifier	Unique value that is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The port used to establish the connection to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port used to establish the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose **Out** (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node	

Field	Description
	to the destination endpoint.

Field	Description	
	Remote Tunnel IP	For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Multi Tunnel	Enable the multi-tunnel flag to create multiple tunnels for flow distribution to the 5G-Cloud application. Refer to 5G-Cloud Ericson SCP Support. **Applicable Platforms**: OpenStack, Third Party Orchestration, VMware ESXi **Notes:** ▪ You can configure either a single-tep or multi-tep setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session. ▪ When you enable Multi-Tunnel on a VXLAN tunnel and set the number of tunnels, GigaVUE-FM automatically creates the additional VXLAN tunnel endpoints. Any later changes to the original VXLAN tunnel, such as disabling Multi-Tunnel or modifying Domain Tagging do not update these auto created endpoints. They continue to retain the configuration that existed at the time they were created.

Field	Description	
		To apply updated settings, you must delete the VXLAN TEP and the associated LB application, then recreate the LB and VXLAN TEP with the new configuration, and re-establish the link between them.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. **Note:** This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to PCAPng Application for details.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose **In** (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It routes the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		

Field	Description	
Note: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to the Secure Tunnels.		
In	Choose **In** (decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
Out	Choose **Out** (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP	For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. **NOTE:** This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to

Field	Description	
		PCAPng Application for details.
ERSPAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	**IP Version**	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. **Note**: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the **Configure Physical Tunnel** option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to Secure Tunnels section.		

Field	Description	
In	**IP Version**	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments for a delay.

Field	Description	
Out	**IP Version**	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that helps network devices identify the higher or lower priority to handle traffic. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable the receipt of acknowledgments.
	Sync Retries	Enter the number of times you can try the sync. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable the receipt of acknowledgments when there is a delay.
UDP:		

Field	Description	
Out	**L4 Destination IP Address**	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. For details, refer to Application Metadata Exporter.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

Create Raw Endpoint (Azure)

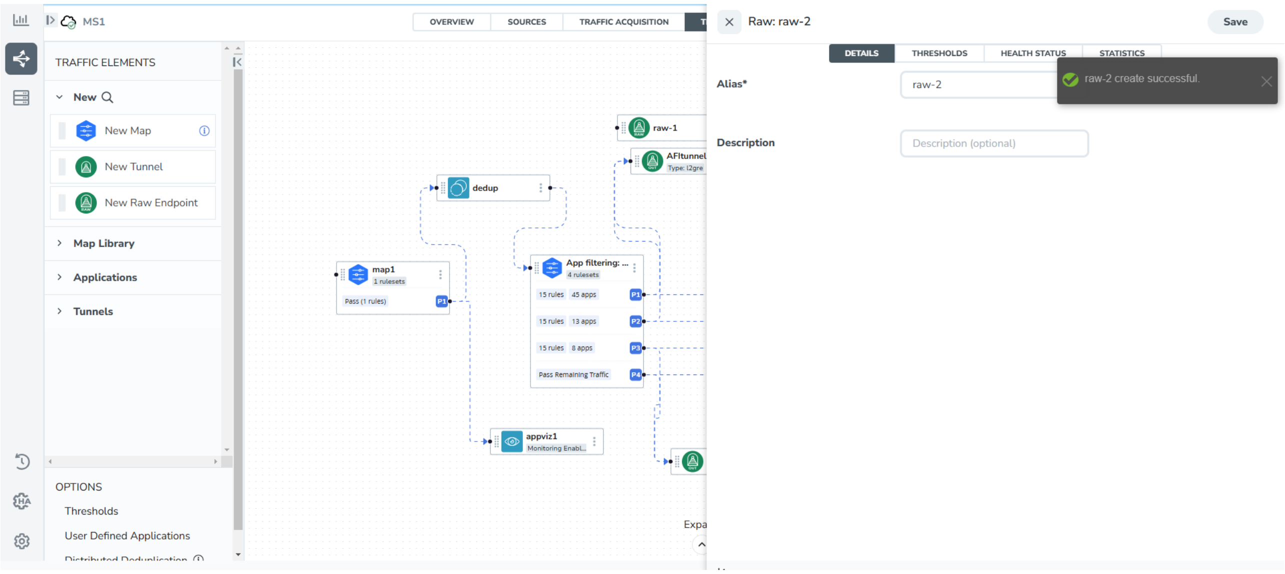
Raw End Point (REP) is used to pass traffic from an interface. REP is used to ingress data from a physical interface attached to GigaVUE V Series Nodes. You can optionally use this end point to send traffic to the applications deployed in the Monitoring Session.

> **NOTE:** The maximum number of links that can egress from any endpoint in V Series is four.

To add Raw Endpoint to the Monitoring Session:

1. Drag and drop **New Raw Endpoint** from the **New** expand menu to the graphical workspace.
2. On the new raw endpoint icon, click the ⋮ menu button and select **Details**. The **Raw** quick view page appears.

3. Enter the Alias and Description details for the Raw End Point and click **Save**.



Alias* raw-2

Description Description (optional)

raw-2 create successful.

4. To deploy the Monitoring Session after adding the Raw Endpoint:
   a. Select **Deploy** from the **Actions** drop-down list on the **TRAFFIC PROCESSING** page. The **Deploy Monitoring Session** dialog box appears.
   b. Select the V Series Nodes for which you wish to deploy the Monitoring Session.
   c. Select the interfaces for each of the REPs and the TEPs deployed in the Monitoring Session from the drop-down menu for the selected individual V Series Nodes.
   d. Select **Deploy**.
5. Select **Export** to download all or selected V Series Nodes in CSV and XLSX formats.

Create a New Map (Azure)

Terms to know before creating a map:

Parameter	Description
Rules	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic.
Priority	Priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority.
Pass	The traffic from the virtual machine is passed to the destination.
Drop	The traffic from the virtual machine is dropped when passing through the map.
Traffic Filter Maps	A set of maps that are used to match traffic and perform various actions on the matched traffic.
Inclusion Map	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ Inclusion Maps - Exclusion Maps** Below are the filter rule types that work in ATS: • mac Source • mac Destination • ipv4 Source • ipv4 Destination • ipv6 Source • ipv6 Destination • VM Name Destination • VM Name Source • VM Tag Destination • VM Tag Source The traffic direction is as follows: • For any rule type as Source - the traffic direction is egress. • For Destination rule type - the traffic direction is ingress. • For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. **Note**: • If no ATS rule filters listed above are used, all VMs and vNICS are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC. • Use the **GigamonNode** Tag to exclude any Gigamon devices from the target. • When using VM Name filter for selecting the Virtual Machines using Inclusion and Exclusion Maps, wild- cards in VM names are not supported. You must use the prefix of the Virtual Machine name.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

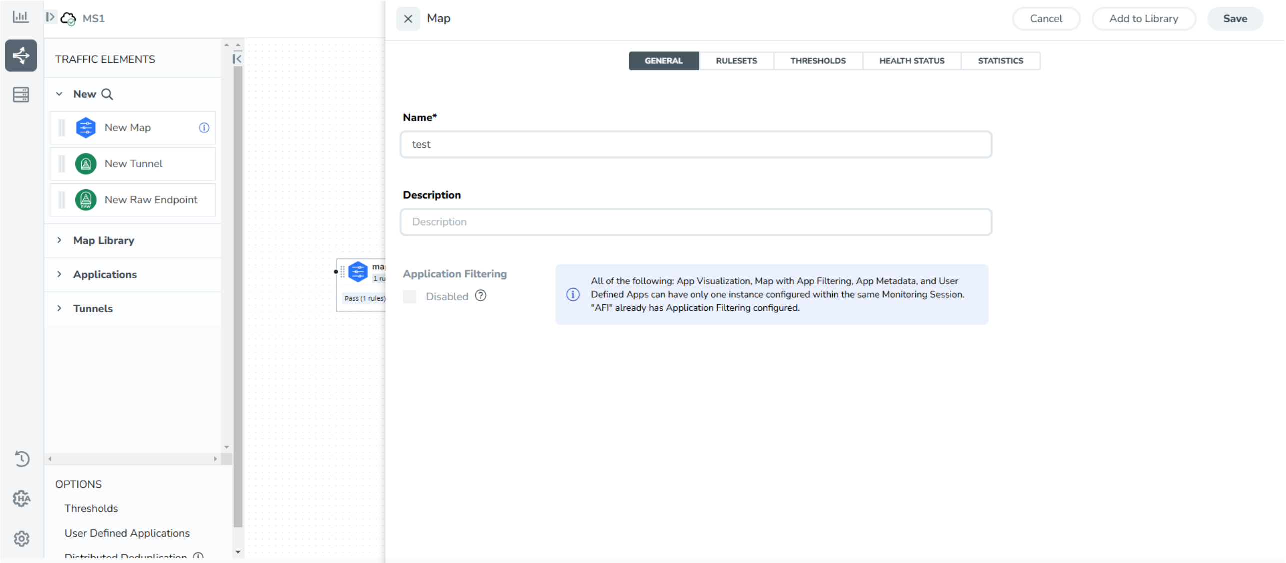
Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.
- Loopback captures bidirectional traffic from both ingress and egress. To prevent duplicate tapping, only egress tapping is permitted.

- If a packet is fragmented then all the fragments are destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM. For details, refer to "Review Map Statistics with Map Rule Counters" section in *GigaVUE Fabric Management Guide*.

To create a new map:

1. Drag and drop **New Map** from the **New** expand menu to the graphical workspace. The **Map** quick view appears.



Name*: test

Description: Description

Application Filtering
□ Disabled

All of the following: App Visualization, Map with App Filtering, App Metadata, and User Defined Apps can have only one instance configured within the same Monitoring Session. "AFI" already has Application Filtering configured.

2. On the new Map quick view, select the **General** tab and enter the required information as described below.
   a. Enter the **Name** and **Description** of the new map.
   b. Enable the **Application Filtering** option if you wish to use Application Filtering Intelligence.
   Enabling this option allows you to filter traffic based on Application name or family. Refer to Application Filtering Intelligence.

> **NOTE:** Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:
> - Traffic Map—Only Pass rules for ATS
> - Inclusion Map—Only Pass rules for ATS
> - Exclusion Map—Only Drop rules for ATS

3. Select the **Rule Sets** tab.
    a. **To create a new rule set:**
        i. Select **Actions > New Ruleset**.
        ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
        iii. Enter the Application Endpoint in the Application EndPoint ID field.
        iv. Select a required condition from the drop-down list.
        v. Select the rule to **Pass** or **Drop** through the map.
    b. **To create a new rule:**
        i. Select **Actions > New Rule**.
        ii. Select a required condition from the drop-down list. Click … and select **Add Condition** to add more conditions.
        iii. Select the rule to **Pass** or **Drop** through the map.
4. Select **Save**.

Through the map, you can drop or pass packets based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. For details, refer to Example- Create a New Map using Inclusion and Exclusion Maps .

You can also perform the following action in the Monitoring session canvas.

- To edit a map, select the ⋮ menu button of the required map on the canvas and click **Details**, or select **Delete** to delete the map.
- To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, select on the Thresholds tab. For more details on how to create or apply threshold templates, refer to Monitor Cloud Health.
- Hover over the rules and apps buttons on the map to view the rule and applications configured for the selected map. Select the rules and apps buttons to open the quick view menu for RULESETS.

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a Monitoring Session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

1. Drag and drop a new map template to the workspace. The New map quick view appears.
2. In the **GENERAL** tab, enter the name as Map 1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.
3. Select the condition as VM Name and enter the **target**. This includes the instances target-1-1, target-1-2, target-1-3, target-2-1, and target-2-2.
4. Select the Expand icon at the bottom of the Monitoring session canvas. The Inclusion Maps and Exclusion Maps section appears.
5. Drag and drop a new map template to the Inclusion Maps region. The New Map quick view appears. Enter the Name and Description of the map.
   a. In the **GENERAL** tab, enter the name as Inclusionmap1 and enter the description. In the **RULESETS**, enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1**. Then, the instance with VM name **target-1-1, target-1-2,** and **target-1-3** is included.
6. Drag and drop a new map template to the Exclusion Maps region. The New Map quick view appears. Enter the details as mentioned in the above section.
   a. In the **GENERAL** tab, enter the name as Exclusionmap1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.
   b. Select the condition as VM Name and enter the VM Name as **target-1-3**. Then, the instance **target-1-3** is excluded.

   Based on this configuration, the Automatic Target Selection selects the instances target-1-1 and target-1-2 as target.

Map Library

Map Library is available in the **TRAFFIC PROCESSING** canvas page. You can add and use the maps from the Monitoring Session.

To add a map,

1. From the **Monitoring Session** screen, select **TRAFFIC PROCESSING**.

   The GigaVUE-FMCanvas page appears.

2. From the page, select the desired map and save it as a template.

3. Select **Details**.

   The Application quick view appears.

4. Select **Add to Library** and perform one of the following:

   - From the **Select Group** list, select an existing group.

- Select **New Group** to create a new one.

5. In the **Description** field, add details, and select **Save**.

The map is added to Map Library. You can use the added map for all the monitoring sessions.

Reusing a map

From the **Map Library**, drag and drop the saved map.

Add Applications to Monitoring Session (Azure)

GigaVUE Cloud Suite with GigaVUE V Series Node supports the following GigaSMART applications in the GigaVUE-FM canvas:

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Slicing
- Masking
- De-duplication
- Load Balancing
- PCAPng Application
- GENEVE Decap
- Header Stripping
- Application Metadata Exporter
- SSL Decrypt
- GigaSMART NetFlow Generation
- 5G-Service Based Interface Application
- 5G-Cloud Application

For more detailed information on how to configure these application, refer to *GigaVUE V Series Applications Guide*

Interface Mapping (Azure)

You can remap interfaces for individual GigaVUE V Series Nodes within a Monitoring Session.

Note: When using Raw and Tunnel In, Interface Mapping is mandatory before you deploy the Monitoring Session.

To perform interface mapping,

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.

   The **Monitoring Sessions** landing page appears.

2. Navigate to the **V SERIES NODES** tab and select **Interface Mapping**.

   The **Deploy Monitoring Session** dialog box appears.

3. Select the GigaVUE V Series Nodes to which you wish to map the interface.

4. From the drop-down menu of the GigaVUE V Series Nodes, select the interfaces for the following deployed in the Monitoring Session:

   - REPs (Raw Endpoints)

   - TEPs (Tunnel Endpoints)

5. Select **Deploy**.

   NOTE: The updated mappings take effect when deployed.

Deploy Monitoring Session (Azure)

You can deploy the Monitoring Session on all the nodes and view the report.

To deploy the Monitoring Session,

1. **Add components to the canvas**
   Drag and drop the following items to the canvas as required:

   - **Ingress tunnel** (as a source): From the **New** section.
   - **Maps:** From the **Map Library** section.
   - **Inclusion and Exclusion maps:** From the Map Library to their respective section at the bottom of the workspace.
   - GigaSMART **apps:** From the **Applications** section.
   - **Egress tunnels:** From the **Tunnels** section.

2. **Connect components**
   Perform the following steps after placing the required items in the canvas.

   a. Hover your mouse on the map

   b. Select the dotted lines

   c. Drag the arrow over to another item (map, application, or tunnel).

      You can drag multiple arrows from a single map and connect them to different maps.
3. **(Optional) Review Sources**
   Select the SOURCES tab to view details about the subnets and monitored instances.

   The monitored instances and the subnets are visible in orange.

   Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method.
4. **Deploy the Monitoring Session**

   From the **Actions** menu, select **Deploy**.

   After successful deployment on all the V Series Nodes, the status appears as **Success** on the **Monitoring Sessions** page.

View the Deployment Report

You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab.

- When you select the **Status** link, the Deployment Report is displayed.
- When the deployment is incorrect, the Status column displays one of the following errors:
  - **Success:** Not deployed on one or more instances due to V Series Node failure.
  - **Failure:** Not deployed on all V Series Nodes or Instances.

The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

The Monitoring Session Deployment includes two key configuration:

- Interface Mapping
- Tool Exclusion

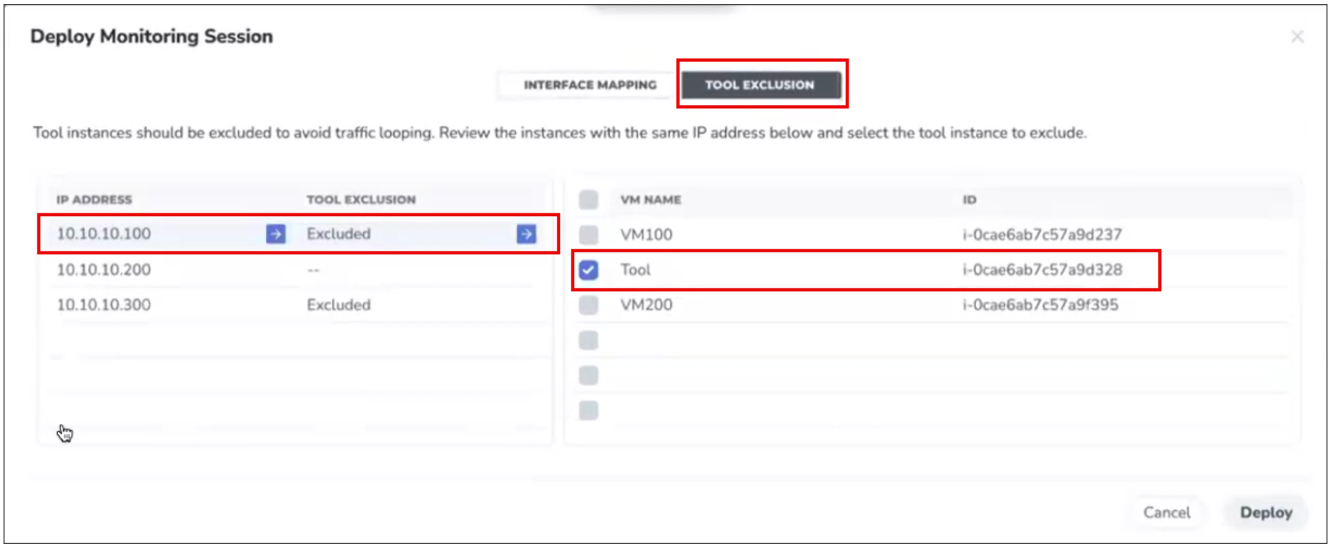
Interface Mapping

It allows to associate specific network interfaces (from monitored instances) with monitoring tools. This ensures that traffic from selected sources is accurately mirrored and routed for analysis. You can:

- Select interfaces from available instances.
- Map each interface to one or more monitoring tools.
- Apply filters or conditions to refine traffic selection.

Tool Exclusion

It excludes specific monitoring tools from receiving mirrored traffic during a monitoring session. This option is available only when the Traffic Acquisition method is set to **VPC Traffic Mirroring**.



Tool instances should be excluded to avoid traffic looping. Review the instances with the same IP address below and select the tool instance to exclude.

IP ADDRESS	TOOL EXCLUSION
10.10.10.100	Excluded
10.10.10.200	--
10.10.10.300	Excluded

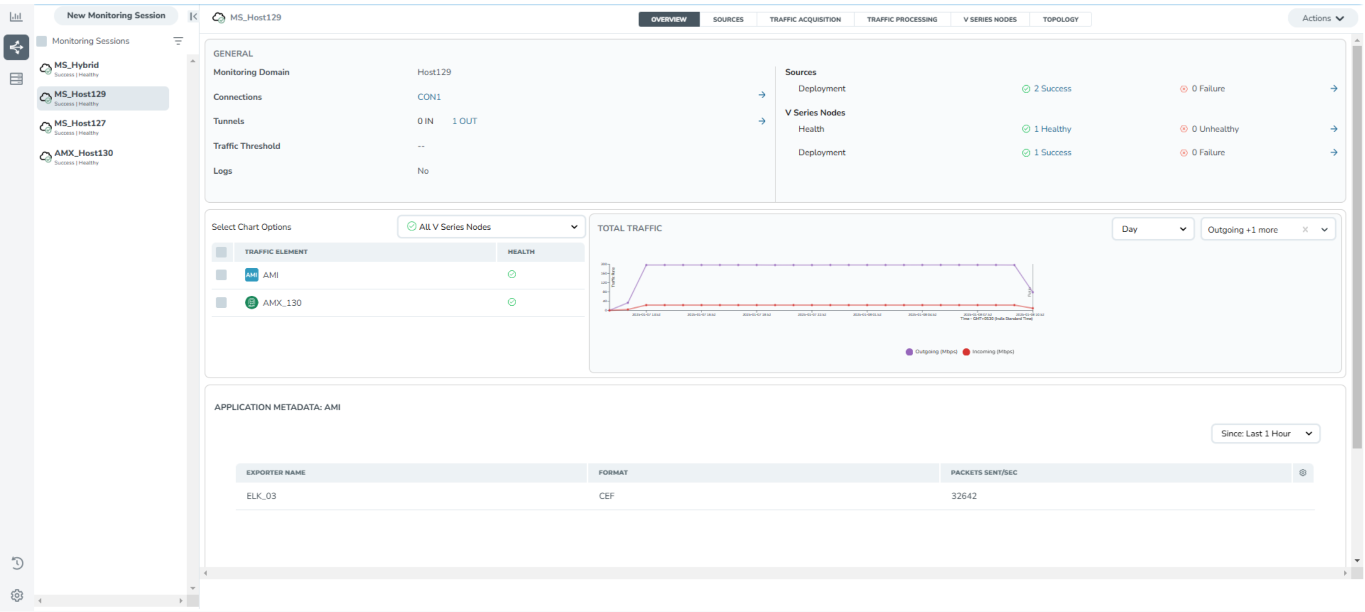
□	VM NAME	ID
□	VM100	i-0cae6ab7c57a9d237
☑	Tool	i-0cae6ab7c57a9d328
□	VM200	i-0cae6ab7c57a9f395

- Review the list of available monitoring tools.
- Select the tools to exclude from traffic flow.
- Confirm the exclusion before deploying the session.

View Monitoring Session Statistics (Azure)

The Monitoring Session **OVERVIEW** page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.

You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab.



GENERAL

Monitoring Domain: Host129

Connections: CON1

Tunnels: 0 IN 1 OUT

Traffic Threshold: --

Logs: No

Sources

Deployment	2 Success	0 Failure

V Series Nodes

Health	1 Healthy	0 Unhealthy
Deployment	1 Success	0 Failure

Select Chart Options: All V Series Nodes

TRAFFIC ELEMENT	HEALTH
AMI	✓
AMX_130	✓

APPLICATION METADATA: AMI

EXPORTER NAME	FORMAT	PACKETS SENT/SEC
ELK_03	CEF	32642

You can view the statistics by applying different filters as per the requirements of analyzing the data. GigaVUE-FM allows you to perform the following actions on the Monitoring Session Statistics page:

- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.
- You can filter the traffic and view the statistics based on factors such as **Incoming**, **Outgoing**, **Ratio (Out/In), Incoming Packets**, **Outgoing Packets**, **Ratio (Out/In) Packets**. You can select the options from the drop-down list box in the **TOTAL TRAFFIC** section of the **OVERVIEW** page.
- You can also view the statistics of the Monitoring Session deployed in the individual V Series Nodes. To view the statistics of the individual GigaVUE V Series Node, select the name of the **V Series Node** for which you want to view the statistics from the GigaVUE V Series Node drop-down list on the bottom left corner of the **OVERVIEW** page.

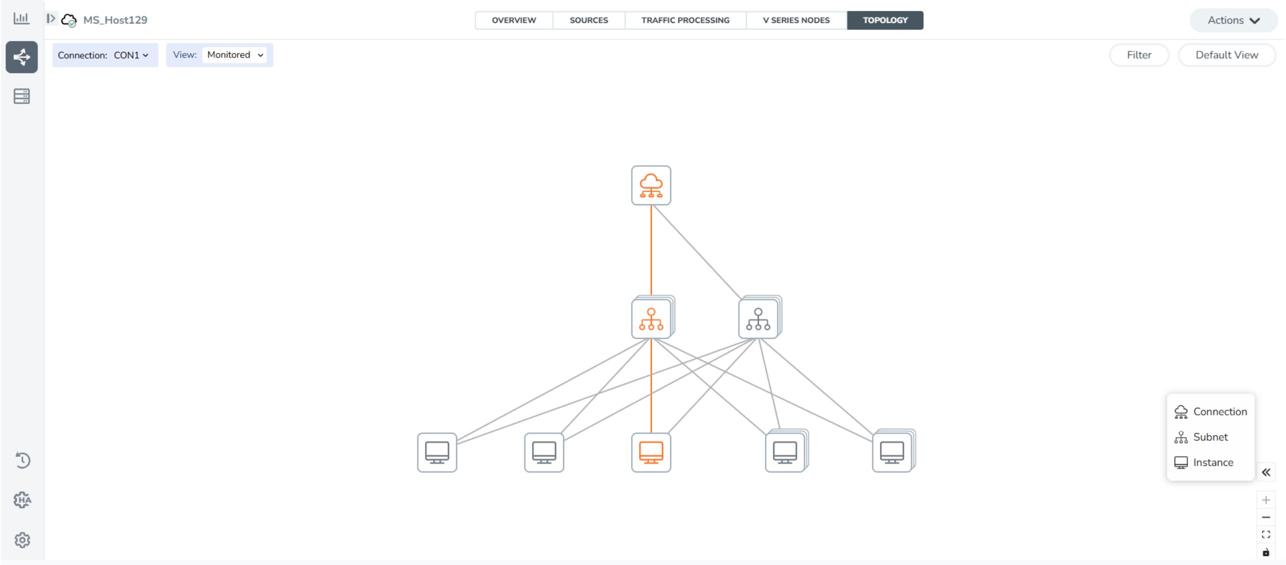
Visualize the Network Topology (Azure)

You can have multiple connections in GigaVUE-FM. Each connection can have multiple Monitoring Sessions configured within it. The Topology tab provides a visual representation of the monitored elements within a selected connection and Monitoring Session.

To view the topology in GigaVUE-FM:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Create a Monitoring Session or select an existing Monitoring Session,
3. Open the **TOPOLOGY** tab.
4. From the **Connection** list on the Topology page, select a connection.

   The topology view of the monitored subnets and instances in the selected session is displayed.
5. From **View,** select one of the following instance types:
   - Fabric
   - Monitored



6. (Optional) Hover over the subnet or VM group icons to view details such as the subnet ID, subnet range, and the total number of subnets and instances.
7. Select the subnet or VM group icons to explore the subnets or instances within the group.

In the Topology page, you can also perform the following:

- Use the **Filter** button to filter the instances based on the VM name, VM IP, OS Type, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitored instances.
- Apply Navigation controls, such as:
  - Use the arrows at the bottom-right corner to move the topology page up, down, left, or right.
  - Use **+** or **-** icons to zoom in and zoom out of the topology view.
  - Select the **Fit View** icon to fit the topology diagram according to the width of the page.

AdditionalInfoAppx

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The VÜE Community

Documentation

©This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

> **NOTE:** In the online documentation, view What's New to access quick links to topics for each of the new features in this Release; view Documentation Downloads to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.13 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide

GigaVUE Cloud Suite 6.13 Hardware and Software Guides
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA400E Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliances Guide
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide
GigaVUE Inline Solutions Guide(**NEW**) (previously included in the **GigaVUE Fabric Management Guide**)
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)

GigaVUE Cloud Suite 6.13 Hardware and Software Guides
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
Universal Cloud TAP - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices Sanitization guidelines for GigaVUE Fabric Management Guide and GigavUE-OS devices.
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **Note**: Release Notes are not included in the online documentation. **Note**: Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software and Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to My Gigamon. Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to My Gigamon.
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

> **NOTE:** My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to: documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	
For Online Topics	**Online doc link**	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*

For PDF Topics	**Document Title**	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	**Describe the issue**	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? **Be as specific as possible.**	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings** ⚙ **> Support > Contact Support** in GigaVUE-FM.

You can also refer to https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)